GUIA GRATUITA

Guia de Seguridad WordPress

Prevencion y Recuperacion ante Ataques e Infecciones

Javier Rivera

Tabla de Contenidos

1 Introducción: Entendiendo las Amenazas

Vamos a aclarar algo desde el principio: cuando tu sitio web recibe un ataque, no es personal. Punto.

Los hackers no se despiertan diciendo "voy a atacar el WordPress de chichorivera". No funciona así. Lo que sucede es que existen mecanismos completamente automatizados que permanentemente están rastreando internet buscando sitios web con vulnerabilidades específicas. Son como máquinas de escaneo que no duermen: buscan versiones desactualizadas de WordPress, plugins vulnerables, configuraciones débiles, directorios expuestos, etc.

¿Cómo funcionan los ataques?

Malwares, Phishing y Spam

- **Malwares:** Son programas maliciosos que infectan tu servidor. Una vez adentro, pueden robar datos, modificar contenido, instalar

puertas traseras, minar criptomonedas con tus recursos, o simplemente destruir tu sitio.

- **Phishing:** Aunque menos común en WordPress, puede dirigirse a los usuarios de tu sitio para robar credenciales. Se presenta como algo legítimo.
- **Spam:** Inyección de contenido malicioso, comentarios spam en masa, o distribución de malware a través de tu sitio.

La realidad de los directorios de vulnerabilidades

Existen bases de datos públicas como:

- **CVE** (Common Vulnerabilities and Exposures)
- **WPScan Vulnerability Database** (específicamente para WordPress)
- **Exploit-DB**

En estas bases de datos están documentadas TODAS las vulnerabilidades conocidas. Cuando sale una nueva versión de WordPress o un plugin, los atacantes automáticos la analizan al instante buscando bugs. Si tu sitio está usando una versión vulnerable, serás detectado y atacado.

> **No es paranoia: es estadística pura.**

¿Cómo exponen los sitios?

Simplemente por:

- **No actualizar** WordPress, plugins o temas
- Dejar **archivos de configuración expuestos** (wp-config.php accesible, readme.html visible)
- Usar **plugins desactualizados** o abandonados
- Tener **usuarios administrador** con nombres predecibles como "admin" o "administrator"

- Contraseñas débiles en **roles críticos**
- Ejecutar **PHP desde carpetas de subidas**
- **XML-RPC habilitado** sin protección

El mito de que "a mí no me atacarán"

Esto es falso. Si tu sitio está indexado por Google, ya forma parte del alcance de los bots atacantes. Estadísticamente, un WordPress desprotegido recibirá intentos de ataque en cuestión de horas, no días.

La solución: Hardening y actualizaciones constantes

No puedes evitar que te busquen, pero sí puedes hacer que no encuentren nada interesante. El "hardening" es exactamente eso: endurecerte contra estos ataques automatizados.

2 Prevención: Antes de que algo suceda

2.1 Mantener todo actualizado (La tarea más importante)

Esto no es opcional. Es como cerrar la puerta de tu casa: es lo mínimo que debes hacer.

WordPress Core:

- Habilita las actualizaciones automáticas si es posible (generalmente ya están activadas)
- Si no, revisa semanalmente si hay nuevas versiones
- Las actualizaciones de seguridad críticas no deberían esperar

Plugins y Temas:

- Elimina TODOS los plugins que no uses, incluso si están desactivados

- Una línea de código que no se ejecuta sigue siendo una vulnerabilidad potencial
- Actualiza regularmente. Los abandonware (plugins sin mantenimiento) son especialmente peligrosos

Herramientas para monitoreo:

- **WPScan:** Escanea tu sitio regularmente detectando versiones vulnerables
- **Wordfence:** Monitoreo en tiempo real de vulnerabilidades
- **Sucuri:** Monitoreo y escaneo de malware

2.2 Respaldos: Tu red de seguridad

> **Aquí viene un detalle importante que muchos hosting no explican bien:**
> Cuando tu hosting dice "Tenemos respaldos diarios, semanales y mensuales", no significa que tengas un histórico. Significa que:
>
> - El respaldo DIARIO de hoy pisa el de ayer
> - El respaldo SEMANAL de esta semana pisa el de la anterior
> - El respaldo MENSUAL de este mes pisa el del mes anterior
>
> **En la realidad:** Tienes exactamente 1 respaldo de cada tipo, no un histórico completo.

Políticas de respaldo recomendadas:

1. **Respaldos incrementales diarios:** Desde tu hosting o con una herramienta
2. **Respaldos completos semanales:** Archivo + base de datos
3. **Respaldos "congelados" mensuales:** Copias que NO sobrescriben automáticamente

4. **Almacenamiento externo:** Guarda copias en Google Drive, Dropbox, un servidor externo, etc.

> **Nunca confíes en UN solo respaldo. Nunca.**

Herramientas de respaldo:

- **UpdraftPlus:** Fácil, integrado en WordPress, con almacenamiento en la nube
- **BackWPup:** Gratuito y potente
- **Duplicator:** Útil tanto para respaldos como para migraciones
- **Respaldos manuales via cPanel/Plesk:** Descarga periódica de archivos + SQL

2.3 Hardening de configuración

2.3.1 Ocultar información sobre WordPress

Edita `wp-config.php` y agrega:

PHP - wp-config.php

```php
// Desactiva edición de plugins y temas desde el dashboard
define('DISALLOW_FILE_EDIT', true);

// Oculta la versión de WordPress
define('WP_CONTENT_URL', 'https://tudominio.com/content');
define('WP_CONTENT_DIR', dirname(__FILE__) . '/content');

// Mejora de seguridad en header
define('DISABLE_FILE_EDIT', true);
```

Elimina `readme.html`: Este archivo expone la versión exacta de WordPress.

```bash
rm readme.html
rm license.txt
```

2.3.2 Desactivar XML-RPC

XML-RPC permite que aplicaciones externas se conecten a tu WordPress. También es vector de ataque para inyecciones.

Opción 1: Agregando a `.htaccess`:

```apache - .htaccess
<Files xmlrpc.php>
    Order Allow,Deny
    Deny from all
</Files>
```

Opción 2: Instala **Disable XML-RPC**

2.3.3 Cambiar URL de administración

El admin está en `/wp-login.php` por defecto. Los atacantes lo saben.

Herramientas:

- **WPS Hide Login:** Gratuito, fácil. Simplemente define una nueva URL para acceder al admin.
- **iThemes Security:** De pago, pero ofrece mucho más.

2.3.4 Limitar intentos de login

Los ataques de fuerza bruta prueban miles de contraseñas por segundo.

Herramientas:

- **Limit Login Attempts Reloaded:** Gratuito, funciona perfecto. Bloquea después de X intentos fallidos.
- **Wordfence:** Versión premium con protección avanzada.

2.3.5 Two-Factor Authentication (2FA)

Una contraseña fuerte es necesaria pero no suficiente.

Herramientas:

- **WP 2FA:** Gratuito, usa autenticador de teléfono o email
- **Two Factor Authentication:** Plugin simple pero efectivo
- **Wordfence:** También lo incluye en su versión premium

2.3.6 Bloquear ejecución de PHP en directorios específicos

Los atacantes suben archivos .php a `/wp-content/uploads/` para ejecutarlos.

En `.htaccess` en la carpeta `/uploads/`:

```
Apache - .htaccess

<FilesMatch "\\.php$">
    Deny from all
</FilesMatch>
```

O más específico:

```
Apache - .htaccess
```

```
<Files ~ "\\.php$">
    deny from all
</Files>
```

2.3.7 Proteger wp-config.php

En `.htaccess` (raíz de WordPress):

```
Apache - .htaccess

<Files wp-config.php>
    Order allow,deny
    Deny from all
</Files>
```

2.3.8 Nombres de usuario seguros

Nunca uses "admin", "administrator", o "adminuser".

Durante la instalación, crea un usuario con nombre único. Si heredaste un sitio con usuario "admin", crea uno nuevo con permisos admin y **elimina el usuario admin**.

2.3.9 Contraseñas fuertes

Mínimo 16 caracteres, mezcla de mayúsculas, minúsculas, números y caracteres especiales.

Herramientas:

- **LastPass Generator**
- **1Password**
- Simplemente: Usa una frase larga y única

2.3.10 Headers de seguridad HTTP

Agrega a tu `.htaccess`:

```
Apache - .htaccess

# Prevenir clickjacking
Header always append X-Frame-Options "SAMEORIGIN"

# Prevenir MIME type sniffing
Header always append X-Content-Type-Options "nosniff"

# Habilitar XSS protection
Header always append X-XSS-Protection "1; mode=block"

# HTTPS redirect
Header always set Strict-Transport-Security "max-age=31536000; incl
```

O puedes usar plugins como **WP Super Cache** o **Sucuri** que lo hacen automáticamente.

2.4 Suite de seguridad recomendada (Mi preferencia personal)

He trabajado con herramientas de pago y gratuitas. Las de pago ofrecen un panel unificado, pero estas gratuitas son igual de efectivas si las combinas:

1. **Sucuri Security** - Hardering, escaneo de malware, monitoreo, notificaciones
2. **Limit Login Attempts Reloaded** - Protección contra fuerza bruta
3. **WP 2FA** - Autenticación de dos factores
4. **Disable XML-RPC-API** - Desactiva XML-RPC
5. **WPS Hide Login** - Cambia URL del admin
6. **UpdraftPlus** - Respaldos automáticos

Si prefieres una solución unificada de pago:

- **Wordfence Premium:** Todo en uno (firewall, 2FA, backups, escaneo)

- **iThemes Security Pro:** Muy bueno en hardening
- **Sucuri** (también tiene plan de pago): Lo mejor en detección y limpieza de malware

3 Bajo Ataque: Guía paso a paso para recuperación

Tu sitio fue comprometido. No es el fin del mundo, pero necesitas actuar rápido y metódicamente.

Paso A: Respaldo completo del directorio raíz

Antes de hacer cualquier cosa, descarga TODA la estructura de tu sitio. Incluso aunque esté infectado, necesitarás analizarlo después.

```bash
# Vía SFTP
# Descarga todo: /public_html o /www (según tu hosting)

# O vía SSH si tienes acceso
tar -czf backup-infected-$(date +%Y%m%d).tar.gz /home/user/public_h
```

> **Por qué:** Aunque parezca contraproducente descargar malware, necesitarás analizarlo para entender qué pasó. Además, si la limpieza va mal, tendrás de dónde volver.

Paso B: Inspección visual y análisis de archivos sospechosos

¿Qué buscar?

- Archivos con nombres raros (shell.php, up.php, wp-load123.php)
- Archivos PHP en directorios que no deberían tenerlos

- Archivos con fechas de creación reciente (comparar con tu última subida legítima)

Dentro del directorio raíz:

```
Estructura

wp-admin/
wp-includes/
wp-content/
.htaccess  <-- BUSCA AQUÍ
index.php
wp-config.php
[Archivos extraños aquí?]
```

Lo que verás en código malicioso:

```php
PHP - Código Malicioso (Ejemplos)

<?php
// Código ofuscado, comprimido:
eval(base64_decode("SGVsbG8gV29ybGQ="));

// O así:
$code = gzinflate(base64_decode("...largo string..."));
eval($code);

// O con expresiones regulares maliciosas:
preg_replace("/.*\/e", "system($_GET['cmd'])", "");

// O simple ejecución de comandos:
system($_GET['cmd']);
shell_exec($_POST['shell']);
assert($_GET['code']);
```

Herramientas de análisis:

- **VirusTotal:** Sube archivos sospechosos para análisis

- **PHP Sandbox:** Analiza código PHP de forma segura
- **Grep:** Busca patrones maliciosos

```bash
grep -r "eval\|base64_decode\|system\|shell_exec\|assert" /ruta/
grep -r "preg_replace.*\/e" /ruta/
```

Paso C: Limpieza del core de WordPress

Aquí es donde eliminas lo que sabes que debe estar limpio.

Elimina:

1. `/wp-admin/` - Carpeta completa
2. `/wp-includes/` - Carpeta completa
3. Todos los archivos raíz EXCEPTO `wp-config.php` y `.htaccess` (aunque lo revisaremos)
4. `readme.html`, `license.txt`, `wp-json` (si no lo usas)

Revisa especialmente wp-config.php:

```php
// LEGÍTIMO: Solo ves variables de configuración
define('DB_NAME', 'nombrebd');
define('DB_USER', 'usuario');
// ... claves de seguridad

// MALICIOSO: Verás eval, base64_decode, referencias a archivos
eval(base64_decode(...));
include($_GET['file']);
require(__DIR__ . '/malware.php');
```

Si `wp-config.php` tiene código extraño:

- Elimínalo. Edita el archivo y deja solo las configuraciones reales de base de datos.
- Las keys y salts (`AUTH_KEY` , `SECURE_AUTH_KEY` , etc.) puedes regenerarlas en https://api.wordpress.org/secret-key/1.1/salt/

Elimina también .htaccess:

Lo reconstruiremos después. Podría tener reglas maliciosas.

Vía FTP/SFTP:

```
Instrucciones

Conecta con tu cliente FTP favorito (FileZilla, WinSCP)
Navega a /wp-admin/ y /wp-includes/
Elimina ambas carpetas
Elimina: index.php, wp-load.php, wp-settings.php, etc. (los PHP de
Mantén: wp-config.php, .htaccess (para revisión)
```

Vía cPanel File Manager:

```
Instrucciones

cPanel > File Manager
Navega a /public_html
Selecciona wp-admin, clic derecho, Delete
Repite con wp-includes
Elimina archivos PHP de raíz
```

Paso D: Descarga e instalación de WordPress limpio

1. Descarga la última versión desde https://wordpress.org/download/

2. Descomprime en tu computadora
3. **IMPORTANTE:** Antes de subir, elimina la carpeta `wp-content` del ZIP descomprimido. Tú vas a conservar tu `wp-content` (plugins, themes, uploads) ya que probablemente están limpios y contienen tu contenido real.
4. Comprime de nuevo (sin wp-content)
5. Sube via FTP/SFTP a tu servidor
6. Descomprime en el servidor (sobrescribe los archivos eliminados)

```bash
# En servidor via SSH:
cd /home/user/public_html
unzip wordpress-clean.zip
# Esto recrea wp-admin/, wp-includes/, index.php, etc.
```

Paso E: Recreación de estructura y validación

Después de descomprimir:

1. **Verifica que wp-content esté intacto** (debe contener tus plugins y temas)
2. **Verifica wp-config.php** (debe estar ahí y sin cambios)
3. **Revisa .htaccess** (si tiene código malicioso, reemplázalo con uno limpio o elimínalo)

```apache
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.html$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
```

```
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

> **Prueba que todo funciona:**
>
> - Visita tu sitio web: ¿Carga?
> - Intenta acceder a `/wp-admin/`
> - ¿Puedes loguear?

Paso F: Limpieza de plugins, temas y actualizaciones

Ya tienes el core limpio. Ahora limpiamos lo que viene con él.

1. Accede a wp-admin

2. Limpieza de plugins:

- Ve a Plugins > Plugins instalados
- **Desactiva y elimina TODOS** excepto los que realmente uses
- Lánzate: si en 3 meses no has usado un plugin, no lo necesitas
- No tener plugins es mejor que tener plugins sin mantenimiento

3. Limpieza de temas:

- Ve a Apariencia > Temas
- **Mantén solo:**
  - El tema activo
  - Su tema padre (si lo tiene)

- **Elimina todos los demás** (Twenty Twenty-Two, Twenty Twenty-Three, etc.)

4. Actualización manual de plugins:

> **Hack importante:** No confíes completamente en las actualizaciones automáticas en un sitio comprometido.

- Ve a cada plugin
- Si no muestra "actualización disponible", **descárgalo limpio** desde:
  - https://wordpress.org/plugins/nombre-plugin/
  - O desde el repositorio oficial
- Elimina la carpeta del plugin vía FTP
- Sube la versión recién descargada

Ejemplo con WP 2FA:

```bash
# Elimina la versión posiblemente infectada
rm -rf /wp-content/plugins/wp-2fa/

# Descarga y extrae el ZIP limpio, sube vía FTP
# O vía dashboard después de descargar el ZIP
```

5. Actualización de temas:

- Repite el mismo proceso con temas custom
- WordPress.com, GeneratePress, OceanWP, etc., tienen versiones limpias en sus repositorios

Paso G: Auditoría de contenido

Ahora que el core está limpio, revisa si el malware inyectó contenido.

Páginas y Entradas:

- Ve a Entradas > Todas las entradas
- Ve a Páginas > Todas las páginas
- Busca títulos o contenido que **no hayas creado**
- Busca redirecciones: `<meta http-equiv="refresh" ...>`
- Busca contenido oculto (CSS color:white, font-size:0px)

Comentarios:

- Ve a Comentarios
- Busca comentarios spam o maliciosos
- Elimina en lotes si hay muchos

Usuarios:

- Ve a Usuarios > Todos los usuarios
- **Busca usuarios sospechosos:**
  - "admin", "administrator" (deberían haber sido creados por ti)
  - Nombres random como "xyzuser123", "hacker", "test"
  - Usuarios con rol Administrator que no conoces
- **Elimina todos menos los administradores legítimos**
- Si editas un usuario para cambiar su rol a "Suscriptor" sin antes revisar, elimínalo

Medios:

- Ve a Biblioteca de medios

- Busca archivos raros (.php subido como .jpg, archivos con nombres extraños)
- Revisa fechas: ¿Cuándo subiste estos archivos?

Paso H: Hardening avanzado post-infección

Tu sitio fue hackeado una vez. Ahora le vas a poner frenos.

Suite de hardening (Mis recomendaciones):

1. Sucuri Security (Gratuito)

- Instalación: Busca en Plugins > Añadir nuevo
- Te hará un escaneo profundo
- Notificaciones si detecta cambios
- Protección contra malware

2. Limit Login Attempts Reloaded (Gratuito)

- Bloquea después de X intentos fallidos
- Configura: 5 intentos, bloqueo de 30 minutos
- Ver > Historial de intentos de login

3. WP 2FA (Gratuito)

- Genera código TOTP (Google Authenticator, Authy)
- O autenticación por email
- Requiere 2FA en dashboard

4. Disable XML-RPC-API (Gratuito)

- Simplemente desactiva XML-RPC

5. WPS Hide Login (Gratuito)

- Configura nueva URL, ej: `/mi-admin-secreto/`

- Los atacantes no conocerán esta URL
- Guárdala en tu gestor de contraseñas

Instalación rápida:

```
Instrucciones

Dashboard > Plugins > Añadir nuevo
Busca: "Sucuri"
Instala y activa
Repite para los otros plugins
```

Paso I: Mejores prácticas de seguridad permanentes

Ahora que limpiaste, hagamos que no vuelva a pasar.

Archivo/Configuración

Elimina rastros en la raíz:

```
Bash

rm readme.html
rm license.txt
rm wp-cli.yml (si existe)
rm .htaccess.bak (archivos de respaldo)
```

Usuarios

Crea usuario administrador seguro:

- Nombre de usuario: algo único (ej: "j.rivera.admin")
- Email: tu correo real
- Contraseña: 18+ caracteres, random
- Guarda en gestor de contraseñas

Si heredaste usuario "admin":

1. Crea nuevo usuario con rol Administrator (nombre único)
2. Loguea con la nueva cuenta
3. Ve a Usuarios
4. Selecciona el usuario "admin" antiguo
5. Clic en "Eliminar"
6. Transfiere sus entradas a la nueva cuenta

Contraseñas

Para TODOS los roles que tengan acceso:

- Mínimo 16 caracteres
- Mayúsculas, minúsculas, números, símbolos
- Únicas (no reutilices)
- Guarda en 1Password o LastPass

Generador: https://www.random.org/passwords/

Roles y permisos

- **Administrator:** Solo TÚ (máximo, 1 persona más si tienes colaborador)
- **Editor:** Si tienes redactores
- **Author:** Si tienes freelancers de contenido
- **Contributor:** Raramente necesario

Menos permisos = menor riesgo.

Acceso física al servidor

Si tienes acceso SSH:

- Usa clave SSH (no contraseña)

- Desactiva login de root
- Cambia puerto SSH predeterminado (22)

Ejemplo en servidor:

```
SSH - ~/.ssh/config

Host miservidor
    HostName ejemplo.com
    User tuuser
    IdentityFile ~/.ssh/id_rsa
    Port 2222  # Puerto customizado
```

Monitoreo continuo

Con Sucuri:

- Revisa Sucuri Security > Alertas semanalmente
- Si ve cambios raros, investiga

Con Limit Login Attempts:

- Ve a Resultados de intentos
- ¿Ves intentos raros? Investiga

Paso J: Respaldo post-hardening

Ahora que todo está limpio y endurecido, **crea un respaldo de referencia**.

Este será tu "baseline" seguro.

Usa UpdraftPlus:

1. Plugins > UpdraftPlus > Configuración
2. Calendario > Crea respaldo manual
3. Descarga archivo ZIP (Descargar copia)

4. Guarda en múltiples lugares:
    - Tu computadora
    - Google Drive
    - Servidor FTP externo
    - Dropbox

O manualmente:

```bash
# Base de datos
mysqldump -u usuario -p nombrebd > sitio-limpio.sql

# Archivos
tar -czf sitio-limpio-files.tar.gz /home/user/public_html/
```

> **Por qué:** Si en las próximas 48-72 horas vuelve a ser hackeado, sabrás que:
>
> 1. Hay una vulnerabilidad específica en tus plugins
> 2. Alguien tiene acceso FTP/SFTP
> 3. Hay un problema de permisos
>
> No tendrás que empezar desde cero.

4 Monitoreo Continuo y Mejora

Herramientas de escaneo periódico

WPScan (Línea de comandos)

Si tienes acceso SSH a tu servidor:

```bash
# Instalación (si tienes Ruby)
gem install wpscan

# Escaneo básico
wpscan --url https://tudominio.com

# Escaneo profundo (requiere API token gratuito)
wpscan --url https://tudominio.com --api-token TU_TOKEN
```

¿Qué detecta?

- Versión de WordPress desactualizada
- Plugins vulnerables
- Temas vulnerables
- Usuarios enumerables

Regístrate gratis en https://wpscan.com/api para token.

Wordfence (Plugin)

Versión gratuita muy buena:

1. Instala plugin "Wordfence Security"
2. Dashboard > Wordfence > Opciones

3. Habilita: Escaneo de archivos, Firewall

Recibe alertas de:

- Cambios de archivos WordPress
- Plugins vulnerables
- Intentos de login fallidos

Checklist mensual

Cada 30 días:

```
Checklist

[ ] Actualizar WordPress
[ ] Actualizar plugins
[ ] Actualizar temas
[ ] Revisar usuarios activos
[ ] Revisar Sucuri y Wordfence
[ ] Crear respaldo
[ ] Probar restauración de respaldo (al menos cada 3 meses)
```

5 Herramientas de Referencia

Herramienta	Tipo	Costo	Función
Sucuri Security	Plugin	Gratuito	Escaneo de malware
Limit Login Attempts	Plugin	Gratuito	Protección fuerza bruta
WP 2FA	Plugin	Gratuito	Autenticación 2FA
WPS Hide Login	Plugin	Gratuito	Cambiar URL admin

Herramienta	Tipo	Costo	Función
UpdraftPlus	Plugin	Gratuito+	Respaldos
Wordfence	Plugin	Gratuito+	Firewall y escaneo
WPScan	CLI/ Web	Gratuito+	Escaneo de vulnerabilidades
iThemes Security	Plugin	Pago	Suite completa

6 Conclusión

La seguridad de WordPress es un proceso continuo, no un destino.

Recuerda:

- Los ataques NO son personales
- Pero SÍ son inevitables si no te proteges
- Las herramientas son el 20%, la disciplina es el 80%
- Mantener todo actualizado previene el 90% de los ataques

Tu plan de seguridad

1. Hoy: Implementa los 5 plugins básicos
2. Esta semana: Actualiza todo y crea respaldo
3. Este mes: Revisa usuarios, contraseñas y permisos
4. Permanentemente: Actualiza, monitorea y respalda

Porque cuando (no "si", sino "cuando") intenten atacar, estarás listo.