Guía de Buenas Prácticas de Seguridad para Sitios WordPress
Versión: 1.0
Destinatarios: Clientes con sitios WordPress alojados en nuestra plataforma.

Introducción
WordPress es el sistema de gestión de contenidos (CMS) más utilizado del mundo y, debido a su popularidad, también es uno de los principales objetivos de ataques automatizados.
La gran mayoría de las infecciones no ocurren por vulnerabilidades del servidor, sino por alguno de los siguientes motivos:

- WordPress desactualizado.
- Plugins o temas vulnerables.
- Contraseñas débiles o reutilizadas.
- Usuarios comprometidos.
- Plugins o temas descargados desde sitios no oficiales.
- Equipos personales infectados desde donde se administró el sitio.

El objetivo de este documento es brindar recomendaciones para reducir significativamente el riesgo de compromiso de un sitio WordPress y definir un procedimiento de actuación ante un incidente de seguridad.

---

1. Mantener WordPress actualizado
Es la medida de seguridad más importante.
Se recomienda:

- Mantener siempre instalada la última versión estable de WordPress.
- Aplicar las actualizaciones de seguridad tan pronto como estén disponibles.
- No mantener versiones obsoletas del CMS.

Utilizando WordPress Toolkit
Nuestra plataforma incluye **WordPress Toolkit**, que facilita la administración segura del sitio.
Se recomienda:

- Habilitar las actualizaciones automáticas del núcleo (Core).
- Verificar periódicamente que las actualizaciones se hayan aplicado correctamente.
- Revisar el funcionamiento del sitio luego de cada actualización.

---

2. Mantener Plugins y Temas actualizados
Más del 90% de las vulnerabilidades explotadas en WordPress corresponden a plugins o temas.
Se recomienda:

- Actualizar los plugins apenas exista una nueva versión estable.
- Actualizar los temas instalados.
- Eliminar plugins y temas que ya no se utilicen.
- Instalar únicamente los componentes realmente necesarios.

Evitar mantener:

- Plugins abandonados.
- Plugins sin soporte del desarrollador.

- Temas incompatibles con versiones actuales de WordPress.

---

3. Descargar únicamente software oficial

Nunca instalar:

- Plugins "nulled".
- Temas pirateados.
- Versiones modificadas obtenidas desde sitios no oficiales.

Siempre descargar desde:

- WordPress.org
- Marketplace oficial del desarrollador
- Proveedores reconocidos

---

4. Utilizar contraseñas seguras

Todas las credenciales deben ser únicas y diferentes entre sí.

Especialmente:

- WordPress
- cPanel
- FTP / SFTP
- Base de datos
- Correo Webmail

Se recomienda utilizar contraseñas de al menos:

- 16 caracteres.
- Letras mayúsculas.
- Letras minúsculas.
- Números.
- Caracteres especiales.

Nunca reutilizar contraseñas entre distintos servicios.

---

5. Habilitar autenticación multifactor (MFA)

Siempre que sea posible, activar MFA para:

- WordPress
- cPanel
- Correo Webmail
- Paneles administrativos

Esto reduce considerablemente el riesgo de accesos no autorizados aun cuando una contraseña haya sido comprometida.

---

6. Limitar los usuarios administradores

Revisar periódicamente:

- Usuarios existentes.
- Roles asignados.
- Cuentas antiguas.
- Usuarios inactivos.

Eliminar:

- Usuarios que ya no administren el sitio.
- Cuentas de prueba.
- Administradores innecesarios.

Aplicar siempre el principio de **mínimo privilegio**, otorgando únicamente los permisos necesarios para cada usuario.

---

7. Utilizar WordPress Toolkit

Nuestra plataforma incorpora **WordPress Toolkit**, una herramienta que facilita la administración y mantenimiento del sitio.

Entre sus principales funcionalidades se encuentran:

- Detección automática de instalaciones WordPress.
- Actualización del núcleo de WordPress.
- Actualización de plugins y temas.
- Verificaciones de seguridad.
- Administración centralizada de múltiples sitios.
- Copias de seguridad (según configuración).

Se recomienda ingresar periódicamente para verificar el estado general del sitio.

---

8. Escaneo periódico con ImunifyAV+

Nuestra plataforma incorpora **ImunifyAV+**, una herramienta de análisis de malware que permite detectar:

- Malware conocido.
- WebShells.
- Backdoors.
- Archivos modificados maliciosamente.
- Código sospechoso.

Se recomienda revisar periódicamente los resultados de los análisis y atender cualquier alerta generada.

---

9. Eliminar componentes innecesarios

No mantener instalados:

- Plugins deshabilitados.
- Temas sin uso.
- Instalaciones antiguas de WordPress.
- Copias olvidadas del sitio.
- Archivos de instalación.

Cada componente adicional incrementa la superficie de ataque.

---

10. Realizar copias de seguridad

Siempre mantener copias recientes del sitio.

Se recomienda:

- Backup diario de archivos.
- Backup diario de la base de datos.
- Conservar varias versiones históricas.

Además, verificar periódicamente que las copias puedan restaurarse correctamente.

---

11. Utilizar HTTPS
Todos los sitios deben utilizar HTTPS mediante certificados SSL.
Beneficios:

- Protege las credenciales.
- Evita la interceptación de información.
- Mejora el posicionamiento SEO.
- Incrementa la confianza de los visitantes.

---

12. Revisar permisos de archivos
Se recomienda utilizar:
Directorios
755
Archivos
644
Nunca utilizar permisos:
777
Permisos excesivos facilitan que un atacante modifique archivos del sitio.

---

13. Deshabilitar servicios innecesarios
Cuando no sean requeridos, conviene deshabilitar:

- XML-RPC.
- Editor de archivos incorporado en WordPress.
- Plugins de administración remota que no se utilicen.

Esto reduce la superficie de ataque del sitio.

---

14. Monitorear la actividad
Revisar periódicamente:

- Nuevos usuarios.
- Cambios de contraseña.
- Instalación de plugins.
- Cambios en la configuración.
- Actividad administrativa.

Detectar una anomalía rápidamente permite minimizar el impacto de un incidente.

---

15. Revisar el sitio luego de cada cambio
Luego de:

- Actualizar WordPress.
- Instalar plugins.
- Actualizar temas.
- Modificar código.

Se recomienda comprobar:

- Correcto funcionamiento.

- Navegación.
- Formularios.
- Comercio electrónico (si corresponde).
- Rendimiento general.

---

16. Utilizar un Firewall de Aplicaciones Web (WAF)

Nuestra plataforma protege los sitios mediante **ModSecurity**, que ayuda a bloquear una gran cantidad de ataques comunes contra aplicaciones web.

Como capa adicional de seguridad, puede ser recomendable instalar un plugin de firewall (WAF) dentro del propio WordPress, especialmente en sitios con alta exposición a Internet o múltiples administradores.

Algunas opciones recomendadas son:

- **Wordfence Security** (recomendado): incorpora firewall de aplicaciones, escaneo de malware, protección frente a ataques de fuerza bruta, monitoreo de integridad de archivos y alertas de seguridad.
- **Solid Security (antes iThemes Security)**: enfocado en el endurecimiento (hardening) de WordPress, protección de accesos y monitoreo de actividad.
- **Sucuri Security**: ofrece auditoría de seguridad, monitoreo de integridad de archivos y detección de actividades sospechosas. Su WAF completo se encuentra disponible como servicio de pago.

Importante: No se recomienda instalar más de un plugin de seguridad o WAF simultáneamente, ya que pueden producir conflictos, afectar el rendimiento o generar falsos positivos.

La combinación de **ModSecurity** en el servidor junto con un único plugin de seguridad correctamente configurado proporciona una protección adicional frente a numerosos ataques automatizados dirigidos a WordPress.

---

17. Mantener seguros los equipos desde donde se administra el sitio

Muchas infecciones comienzan desde el computador del administrador.

Se recomienda:

- Antivirus actualizado.
- Sistema operativo actualizado.
- Navegador actualizado.
- No almacenar contraseñas en equipos compartidos.
- Utilizar gestores de contraseñas confiables.

---

18. Realizar auditorías periódicas

Al menos una vez por trimestre revisar:

- Usuarios.
- Plugins.
- Temas.
- Permisos.
- Copias de seguridad.
- Versión de PHP.

- Vulnerabilidades conocidas.
- Resultados de ImunifyAV+.

Modelo de Seguridad en Capas

La seguridad de un sitio WordPress no depende de una única herramienta, sino de varias capas de protección que trabajan de forma complementaria.

Capa	Herramienta	Función
Infraestructura	Firewall del proveedor	Protege la red y los servicios del servidor.
Servidor Web	ModSecurity	Bloquea ataques HTTP conocidos, inyecciones SQL, XSS y otras amenazas comunes.
Sistema Operativo	ImunifyAV+	Detecta malware, webshells, backdoors y archivos maliciosos.
Administración	WordPress Toolkit	Facilita la actualización del núcleo, plugins y temas, además de verificaciones de seguridad.
Aplicación	Plugin WAF (Wordfence, Solid Security o Sucuri)	Protección específica para WordPress frente a fuerza bruta, cambios de archivos y otras amenazas.
Usuario	Contraseñas robustas + MFA	Reduce el riesgo de accesos no autorizados por robo o reutilización de credenciales.

Plan de Acción ante una Infección

Si un sitio presenta indicios de haber sido comprometido, recomendamos actuar inmediatamente siguiendo el siguiente procedimiento.

Paso 1. Aislar el problema

Si es posible:

- Colocar el sitio en modo mantenimiento.
- Evitar nuevas modificaciones.
- Preservar la evidencia.

Paso 2. Ejecutar un análisis

Utilizar:

- ImunifyAV+.
- WordPress Toolkit.
- Herramientas de análisis disponibles en la plataforma.

Identificar:

- Archivos infectados.
- WebShells.
- Backdoors.
- Código malicioso.

Paso 3. Cambiar todas las contraseñas

Modificar inmediatamente:

- WordPress.
- cPanel.
- FTP / SFTP.
- Base de datos.
- Correo Webmail.
- SSH (si estuviera habilitado).

Nunca reutilizar las contraseñas anteriores.

Paso 4. Revisar los usuarios

Buscar:

- Administradores desconocidos.
- Usuarios recientemente creados.
- Cambios de permisos.
- Cuentas sospechosas.

Eliminar inmediatamente cualquier usuario no autorizado.

Paso 5. Actualizar todo el software

Actualizar:

- WordPress.
- Plugins.
- Temas.
- PHP.

Paso 6. Eliminar software vulnerable

Eliminar:

- Plugins abandonados.
- Plugins innecesarios.
- Temas vulnerables.
- Componentes sin soporte.

Paso 7. Restaurar archivos afectados

Siempre que sea posible:

- Restaurar desde una copia de seguridad limpia.
- Reemplazar archivos comprometidos por versiones originales.

Paso 8. Ejecutar un nuevo análisis

Una vez finalizada la limpieza:

- Ejecutar nuevamente ImunifyAV+.
- Confirmar que no existan archivos maliciosos remanentes.

Paso 9. Revisar los registros

Analizar:

- Accesos recientes.

- Direcciones IP.
- Intentos de autenticación.
- Cambios realizados.
- Archivos modificados.

Esto ayuda a identificar el origen del incidente y evitar futuras infecciones.

Paso 10. Verificar el funcionamiento

Comprobar:

- Navegación.
- Panel administrativo.
- Formularios.
- Carga de imágenes.
- Comercio electrónico (si corresponde).
- Integraciones externas.

Paso 11. Fortalecer la seguridad

Luego del incidente se recomienda:

- Activar MFA.
- Cambiar todas las contraseñas.
- Eliminar componentes innecesarios.
- Habilitar las actualizaciones automáticas.
- Revisar permisos de archivos.
- Verificar que ModSecurity permanezca habilitado.
- Considerar la instalación de un plugin WAF si aún no se utiliza.

Herramientas de Seguridad Disponibles en Nuestra Plataforma

Como parte de nuestros servicios de hosting, los clientes disponen de diversas herramientas para fortalecer la seguridad de sus sitios WordPress.

Herramienta	Función
WordPress Toolkit	Administración centralizada de WordPress, actualización del núcleo, plugins y temas, verificaciones de seguridad y administración del sitio.
ImunifyAV+	Escaneo de malware, detección de webshells, backdoors y archivos maliciosos.
ModSecurity	Firewall de aplicaciones web (WAF) que protege el sitio frente a ataques HTTP comunes.
Backups	Restauración de versiones anteriores del sitio (según el plan contratado).
HTTPS / SSL	Protección de las comunicaciones mediante cifrado.
Monitoreo de infraestructura	Supervisión continua de la plataforma de hosting.

Recomendaciones Finales

La seguridad de un sitio WordPress es un proceso continuo y una responsabilidad compartida entre el proveedor de hosting y el administrador del sitio.

Nuestra plataforma incorpora diversas capas de protección, incluyendo **ModSecurity**, **ImunifyAV+**, **WordPress Toolkit**, copias de seguridad y monitoreo de infraestructura. Sin embargo, la actualización periódica de WordPress, plugins y temas, el uso de contraseñas robustas, la activación de autenticación multifactor, la eliminación de componentes innecesarios y la revisión frecuente del sitio siguen siendo fundamentales para mantener un entorno seguro.

Ante cualquier comportamiento inusual, como redirecciones inesperadas, aparición de usuarios desconocidos, cambios no autorizados o alertas de malware, recomendamos contactar de inmediato a nuestro equipo de soporte para realizar un análisis y aplicar las medidas correctivas correspondientes.