4.2. Seguridad en Wordpress

Conceptos generales sobre seguridad

Desde el panel de administración del Wordpress hay que:

- Mantener **actualizado** Wordpress, Plugins y Temas.
- Tener responsabilidad en la elección e instalación de Plugins y Temas:
  - Instalar sólo plugins que estén registrados en el repositorio oficial de plugins de Worpdress disponible en https://es.wordpress.org/plugins/
  - Conviene encarecidamente realizar búsquedas en Internet sobre posibles vulnerabilidades.
- Instalar y configurar adecuadamente varios plugins de seguridad.
- NOTA: En un Wordpress de wordpress.com no hay que preocuparse de estos puntos, ya que desde wordpress.com se encargan de mantener actualizado el worpdress y sólo usan plugins validados por ellos.

Pero también es necesaria la **involucración** de los usuarios del Wordpress:

- Los usuarios deben usar **contraseñas complejas**.
- No dejarse sesiones abiertas en navegadores.

Y sobre todo, hay que tener **copia de seguridad de todo**. *Si de algo no tienes copia de seguridad, quizás sea porque no te importa mucho perderlo...*

Medidas de seguridad esenciales para Wordpress

Copyright 2026

- No hay que tener un usuario llamado **admin,** ni un usuario llamado igual que nuestro Wordpress, ya que será el primer usuario que intenten probar para hackear el Wordpress. Otros nombres no recomendados: administrador, wp, wordpress, etc.
- Ocultar los nombres de los usuarios haciendo que cada usuario tenga un "alias" para mostrar diferente de su "nombre de usuario", lo cual se configura en el perfil de cada usuario.
- Instalar y configurar **Wordfence** (es un plugin completo: escaner y cortafuegos), para realizar escaneos de posibles ataques (actúa como medida de detección y limpieza de malware) y para bloquear conexiones detectadas como maliciosas (actúa como cortafuegos).
- El plugin **Captcha by Bestwebsoft** añade un captcha en la página de login. Un captcha solicita que se introduzca letras o números, con interacción con el usuario, para evitar múltiples intentos de acceso automáticos. Tiene opción de bloqueo de acceso ante errores de login, lo mismo que en Wordfence: Se pueden tener las dos en paralelo, y se aplicará el bloqueo que se dé en primer caso.
- Realizar **copias de seguridad** del Wordpress con UpdraftPlus y guardarlas, por ejemplo en Dropbox.
- El plugin **Really Simple SSL** es MUY interesante, ya que con él se puede activar la conexión segura **https** para tu Wordpress. Si el servidor de alojamiento no tiene conexión segura, la dirección de acceso a tu Wordpress será del estilo

  http://nombredelwordpress.es, y los navegadores marcarán tu sitio Wordpress como un sitio no confiable. En tal caso será muy recomendable que instales y actives el plugin Really Simple SSL, y la dirección de acceso a tu Wordpress será del estilo

  https://nombredelwordpress.es y los navegadores marcarán tu sitio Wordpress como un sitio confiable.

Recomendable:

- Es muy recomendable instalar y configurar **All in One WP Security**, que es un completo plugin de seguridad. Tiene algunas funcionalidades repetidas con Wordfence, en tales casos sólo convendría tener activadas dichas funcionalidades en uno de los dos plugins.
- **Anti-Malware Security and Brute-Force Firewall**: Escaneo sencillo pero efectivo para detectar hackeos en el Wordpress.
- **Plugin Security Scanner:** Permite revisar vulnerabilidades en tus otros plugins.

Copyright 2026

Recuperar un Wordpress hackeado (requiere acceso al alojamiento web)

Aun con todo, existen listados de vulnerabilidades conocidas de Wordpress, Plugins y Temas: https://wpvulndb.com/, y cada día van saliendo nuevas vulnerabilidades. En los siguientes enlaces encontraremos más información sobre qué hacer con un Wordpress hackeado:

https://codex.wordpress.org/FAQ_My_site_was_hacked

https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/

A modo de prevención, estas webs serán muy útiles para Administradores informáticos en busca de vulnerabilidades:

- https://wpscans.com/
- https://wpscan.org/

Revision #5
Created 2022-04-25 08:30:01 CEST by Equipo CATEDU
Updated 2022-06-29 13:28:16 CEST

Copyright 2026