



WordPress no necesita plugins de seguridad

Aunque a veces ayudan...

Si te vas a dedicar a Internet

has de conocer cómo funciona Internet (al menos un poco).

¿Es WordPress seguro?



Sí

Creo que lo puedo decir más alto, pero no más claro.

Vayamos por partes

WordPress es seguro, sí, pero ¿qué es WordPress?

WordPress está formado por varias partes:

- Alojamiento (servidor, PHP, base de datos...)
- WordPress (núcleo)
- Plugins
- Themes
- Otras cosas

¿Es todo lo de WordPress seguro?

Ahora sí, la respuesta es NO.

Aunque el núcleo de WordPress es seguro, hay otros elementos externos que no lo son.

NOTA: La seguridad al 100% es mentira, no existe ni se la espera. Cuando hablamos de "seguro" es porque las vulnerabilidades se corrigen rápidamente tras conocerse.

¿Podemos reducir los riesgos?

Sí.

Y para ello vamos a revisar cada uno de los elementos que hemos comentado antes.

Comencemos por el principio.

Érase una vez un jovencito confuso que andaba por unas islas...

Alojamiento web

El alojamiento web

El alojamiento web es la casa de tu web.

- Buen soporte técnico
- Buena atención al cliente

¿Eres técnico?

- Control absoluto (*root*)

Imprescindible:

- Sistema contra ataques DDoS
- Firewall + WAF

El alojamiento web

Requisitos muy mínimos:

- PHP 7.2+
- MySQL 8.0+ | MariaDB 10.2+
- Apache 2.4+ | nginx 1.12+

Mantén al día el servidor según los requisitos mínimos de WordPress:
<https://wpalojamiento.com/requerimientos/>

Ahora instalamos WordPress

¿Es seguro?

Sí, pero se puede **mejorar**.

¡Veamos cómo!

WordPress

Siempre HTTPS

Como mínimo en los paneles:

```
define('FORCE_SSL_LOGIN', true);  
define('FORCE_SSL_ADMIN', true);
```

Y así evitarás chafarderos...



Bloquea el PHP en los uploads

¿Para qué necesitas que se ejecuten PHP?

```
<Files ~ ".+\.php">  
    Deny from all  
</Files>
```



Con Apache HTTPD, dentro del fichero .htaccess en la carpeta [/wp-content/uploads/].

Elimina cabeceras inconvenientes

```
remove_action('set_comment_cookies', 'wp_set_comment_cookies');
add_filter('show_admin_bar', '__return_false');
add_filter('the_generator', '__return_false');
remove_action('wp_head', 'adjacent_posts_rel_link', 10, 0);
remove_action('wp_head', 'adjacent_posts_rel_link_wp_head', 10, 0);
remove_action('wp_head', 'feed_links', 2);
remove_action('wp_head', 'feed_links_extra', 3);
remove_action('wp_head', 'rsd_link');
remove_action('wp_head', 'wlwmanifest_link');
remove_action('wp_head', 'wp_generator');
remove_action('wp_head', 'wp_shortlink_wp_head', 10, 0);
```

Elimina cabeceras inconvenientes

Hagámoslo fácil

<https://code.wpdanger.com/wp-content/uploads/wpdanger-headers.zip>

Subid este plugin por FTP a la carpeta [/wp-content/mu-plugins/] y ¡ya está! 😊

Con eso "eliminamos basurilla" que por defecto no es necesaria.

¡Actualiza!

Lo más importante...

...para la seguridad de WordPress es que todo esté al día.

Y cuando digo todo es TODO.

Así que, ¡ACTUALIZA!

NOTA: Sé que soy muy pesado con esto de actualizar, pero, por si no te ha quedado claro, AC_TUA_LI_ZA.

Themes

La elección del theme

Lo que sé ve es menos importante que lo que no se ve.

Buah lo que ha dicho... ¡Ahora vas y lo tuiteas!

- Que se vaya actualizando con **frecuencia**.
- Última versión de menos de **4 meses**.
- Si es *premium*, busca su sitio **web oficial** y cómprala solo ahí.
- Nunca **descargues** una *premium* fuera de su sitio web.

Los temas hijo

Es importante **no sobrescribir los themes** originales para hacer modificaciones, y para eso tenemos los *child themes* (temas hijo).

En los hijos puede haber solo cambios de estilos (visual) pero si se añade o cambia funcionalidad, cada vez que el padre se actualice, **el hijo debe repasarse**.

Plugins

Regla de oro

Desintoxicacion
de *pluginitis*

*que queda todo hecho una
pocilga.*



La elección del plugin

El plugin perfecto.

- Que se vaya actualizando con **frecuencia**.
- Última versión de menos de **4 meses**.
- Si es *premium* busca su **sitio oficial** y cómpralo solo ahí.
- Nunca **descargues** un *premium* fuera de su sitio web.

La elección del plugin

Pero no solo eso, también hay otros factores:

- Que sea compatible con tu versión de PHP.
- Que sea compatible con tu versión de WordPress.

Y ¿por qué es esto importante?

Por ¡WordPress 5.1!

Usuarios

¿Quién anda ahí?

Un usuario se balanceaba sobre la tela de una araña, como veía que no se accedía, fue a buscar a otro... en fin...

Aunque una clave compleja no es lo que te esperas... que seguramente será como...



Contraseña

```
qm2D_Y^z3v#P6HnR=2TD7%rJ%TBLTkK9BwC^
```

Que sí, que esto es complejo.. pero yo me refiero a esto otro..

Contraseña

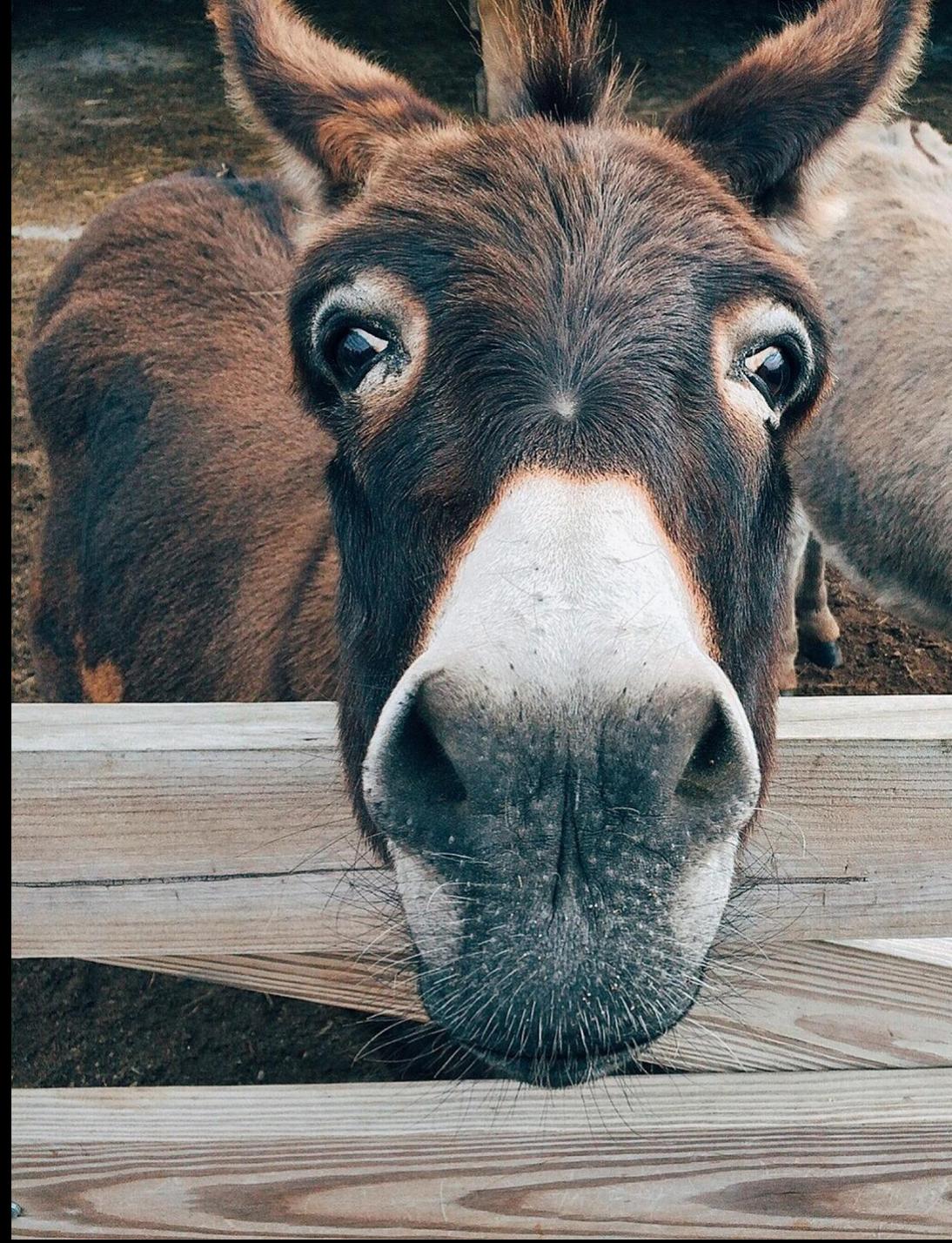
AyerMeFuiAPasearAMiPerroBobbyAlParqueDeAbajo

Esto también es una clave segura (aunque es verdad que no todos los proveedores te dejan poner contraseñas sin números o símbolos).

Venga, un plugin

Two Factor

<https://wordpress.org/plugins/two-factor/>



¿Ya?

Sí, pero no

Estos son elementos muy básicos que te permiten tener un WordPress sin necesidad de plugins de seguridad, pero...

¡ACTUALIZA!

Porque, al fin y al cabo, es la única forma de estar seguro.



Gracias

www.javiercasares.com

javier@casares.org

+Documentación: code.wpdanger.com

+Información: wpalojamiento.com