

White Paper  
**Consejos para securizar la  
instalación de WordPress**



**Hostalia.**

La fama alcanzada por WordPress como CMS para la gestión y desarrollo de páginas web, ha traído consigo que también sea el objetivo de infinidad de ataques. Para evitar posibles hackeos, son muchas las cosas que se pueden llevar a cabo. Debido a la importancia de poder disfrutar de un sitio totalmente seguro, hoy os vamos a dejar algunas recomendaciones que os ayudarán a securizar la instalación de **WordPress** y mantenerse de esta forma mejor protegidos.

## **Actualizar WordPress, plugins y plantilla utilizada**

Empezaremos con un clásico que no debemos olvidar jamás. Es muy importante trabajar siempre con la última versión de WordPress que se haya lanzado al mercado. Con esto nos aseguraremos de que las vulnerabilidades detectadas en versiones anteriores se hayan quedado solucionadas.

Además de mantener actualizado el *core* de WordPress, también es importante hacer lo mismo con los plugins que tengamos instalados y con el tema que utilicemos para nuestro diseño.

### Actualizaciones de WordPress

Importante: antes de actualizar, por favor, [haz una copia de seguridad de tu base de datos y archivos](#). Si necesitas ayuda con las actualizaciones visita la página del Codex [«Actualizar WordPress»](#).

Última comprobación el 5 junio, 2019 a las 4:30 pm.

Hay disponible una nueva versión actualizada de WordPress.

Puedes actualizar a [WordPress 5.2.1-es ES](#) de forma automática:

Puedes actualizar a [WordPress 5.2.1-en US](#) de forma automática:

Mientras se actualiza tu sitio permanecerá en modo mantenimiento. Tan pronto como finalicen las actualizaciones tu sitio volverá a su estado normal.

### Plugins

Los siguientes plugins tienen nuevas versiones disponibles. Selecciona los que quieras actualizar y haz clic en «Actualizar plugins».

Seleccionar todos

---

 Akismet Anti-Spam  
Tienes la versión 4.1.1. Actualiza a la 4.1.2. [Ver detalles de la versión 4.1.2.](#)  
Compatibilidad con WordPress 5.1.1: 100% (según su autor)  
Compatibilidad con WordPress 5.2.1: 100% (según su autor)

---

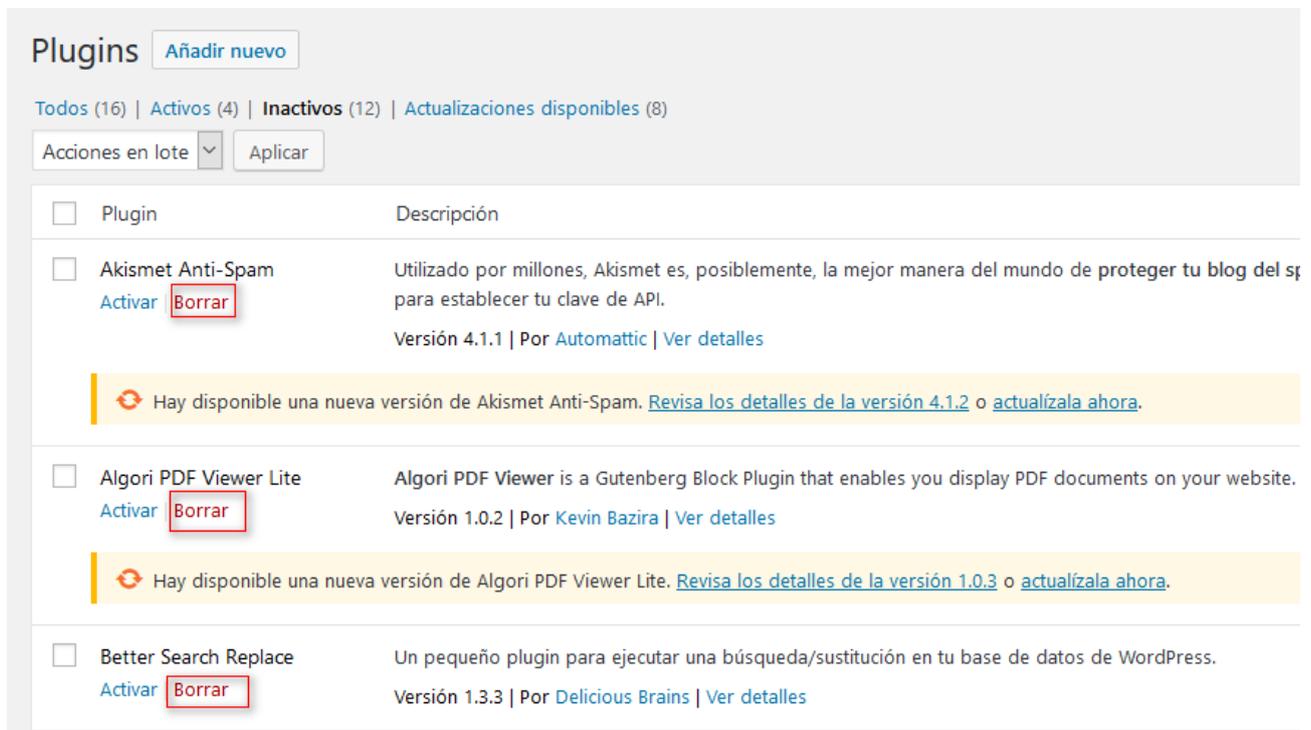
 Algori PDF Viewer Lite  
Tienes la versión 1.0.2. Actualiza a la 1.0.3. [Ver detalles de la versión 1.0.3.](#)  
Compatibilidad con WordPress 5.1.1: 100% (según su autor)  
Compatibilidad con WordPress 5.2.1: 100% (según su autor)

Por suerte, mantener todo esto actualizado no es complicado. WordPress ofrece un sistema de actualizaciones automáticas, tanto para el mismo núcleo de WordPress como para plugins y temas. Eso sí, no os olvidéis de realizar una **copia de seguridad** de vuestra web antes de actualizar, para poder tener la opción de restaurarla en caso de sufrir algún problema durante el proceso de actualización.

## No utilizar plugins o temas obsoletos

De igual forma que es importante tener actualizado WordPress, plugins y temas a la última versión disponible, también lo es no utilizar plugins y temas que se hayan quedado obsoletos y que no se sigan actualizando. Además de poder ser incompatibles con la versión de WordPress, pueden ser un coladero para que los **hackers** realicen sus ataques.

Lo bueno de esto es que el directorio oficial de WordPress retira automáticamente plugins y temas que no se hayan actualizado durante más de dos años, lo que supone una garantía adicional para el usuario.



The screenshot shows the WordPress 'Plugins' management interface. At the top, there's a 'Plugins' header with an 'Añadir nuevo' button. Below it, filters for 'Todos (16)', 'Activos (4)', 'Inactivos (12)', and 'Actualizaciones disponibles (8)' are visible. A dropdown menu for 'Acciones en lote' and an 'Aplicar' button are also present. The main content area lists three plugins, each with a checkbox, a 'Borrar' button (highlighted with a red box), and a description. The first plugin is 'Akismet Anti-Spam', the second is 'Algori PDF Viewer Lite', and the third is 'Better Search Replace'. Each plugin entry also includes a version number and a link to 'Ver detalles'. Below each plugin entry, there is a yellow notification banner indicating that a newer version is available and providing a link to 'actualízala ahora'.

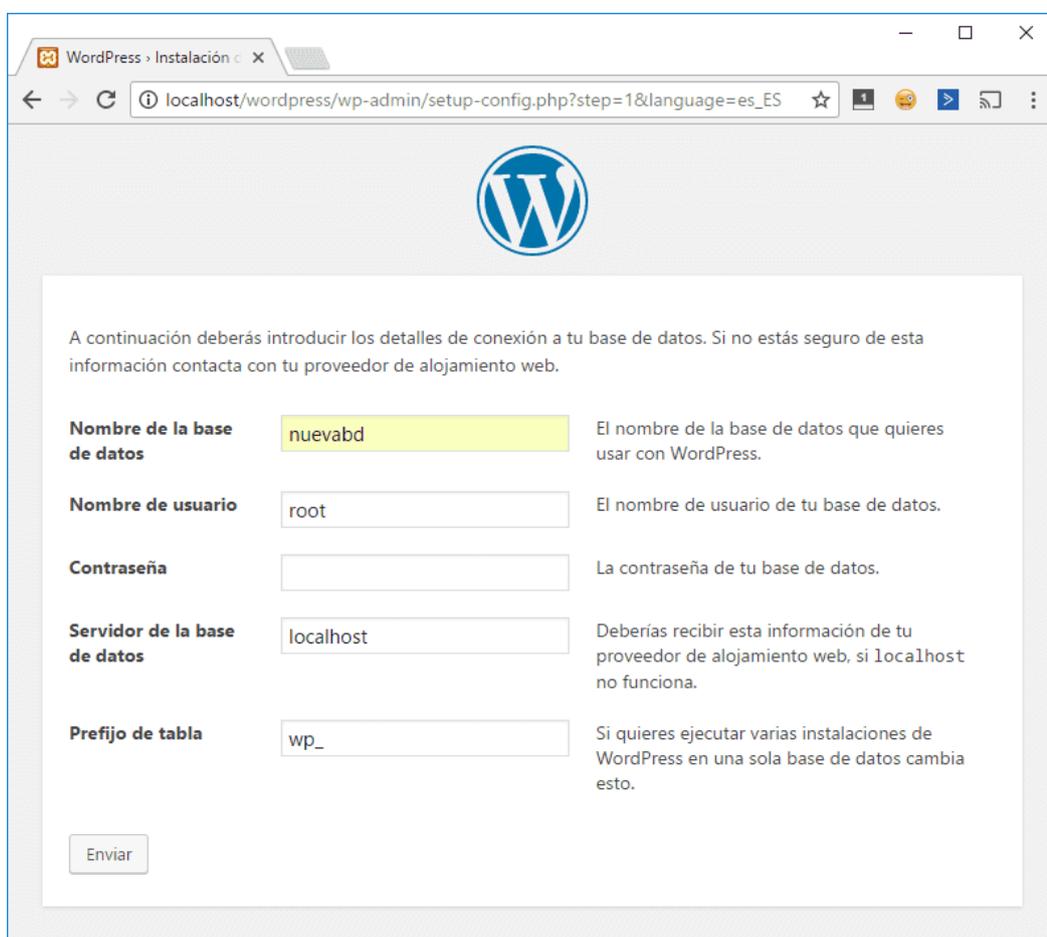
<input type="checkbox"/>	Plugin	Descripción
<input type="checkbox"/>	Akismet Anti-Spam <a href="#">Activar</a> <b>Borrar</b>	Utilizado por millones, Akismet es, posiblemente, la mejor manera del mundo de proteger tu blog del spam para establecer tu clave de API. Versión 4.1.1   Por <a href="#">Automatic</a>   <a href="#">Ver detalles</a>
Hay disponible una nueva versión de Akismet Anti-Spam. <a href="#">Revisa los detalles de la versión 4.1.2</a> o <a href="#">actualízala ahora</a> .		
<input type="checkbox"/>	Algori PDF Viewer Lite <a href="#">Activar</a> <b>Borrar</b>	Algori PDF Viewer is a Gutenberg Block Plugin that enables you display PDF documents on your website. Versión 1.0.2   Por <a href="#">Kevin Bazira</a>   <a href="#">Ver detalles</a>
Hay disponible una nueva versión de Algori PDF Viewer Lite. <a href="#">Revisa los detalles de la versión 1.0.3</a> o <a href="#">actualízala ahora</a> .		
<input type="checkbox"/>	Better Search Replace <a href="#">Activar</a> <b>Borrar</b>	Un pequeño plugin para ejecutar una búsqueda/sustitución en tu base de datos de WordPress. Versión 1.3.3   Por <a href="#">Delicious Brains</a>   <a href="#">Ver detalles</a>

A lo dicho anteriormente, también hay que añadir la práctica de borrar tanto los plugins como los temas que no estemos utilizando. No sólo ocupan espacio en tu **alojamiento** sino que suponen una vía de entrada a posibles vulnerabilidades en tu web.

Todo este proceso de borrado lo podemos hacer desde el propio WordPress, tal y como podemos ver en la imagen superior.

# Cambiar el prefijo de la base de datos

Cuando se realiza una instalación de WordPress desde cero, en uno de los pasos hay que indicar los datos de conexión a la base de datos. Además de indicar el nombre del usuario, nombre de la base de datos y la contraseña, también se nos ofrece la opción de indicar el prefijo de las tablas. Por defecto viene indicado **"wp\_"**, de manera que las tablas quedarán tal que **"wp\_options"**, **"wp\_comments"** o **"wp\_posts"**. Por supuesto, esto es información gratuita que damos a los atacantes, que saben que si se utilizan los valores por defecto, las tablas tendrán ese tipo de nombre.



The screenshot shows the WordPress installation configuration page in a browser. The URL is localhost/wordpress/wp-admin/setup-config.php?step=1&language=es\_ES. The page features the WordPress logo at the top and a form for entering database connection details. The form includes fields for database name, username, password, server, and table prefix, each with a corresponding explanation. The 'Nombre de la base de datos' field is highlighted in yellow and contains the value 'nuevabd'. The 'Nombre de usuario' field contains 'root', 'Servidor de la base de datos' contains 'localhost', and 'Prefijo de tabla' contains 'wp\_'. An 'Enviar' button is located at the bottom left of the form.

A continuación deberás introducir los detalles de conexión a tu base de datos. Si no estás seguro de esta información contacta con tu proveedor de alojamiento web.		
<b>Nombre de la base de datos</b>	<input type="text" value="nuevabd"/>	El nombre de la base de datos que quieres usar con WordPress.
<b>Nombre de usuario</b>	<input type="text" value="root"/>	El nombre de usuario de tu base de datos.
<b>Contraseña</b>	<input type="password"/>	La contraseña de tu base de datos.
<b>Servidor de la base de datos</b>	<input type="text" value="localhost"/>	Deberías recibir esta información de tu proveedor de alojamiento web, si localhost no funciona.
<b>Prefijo de tabla</b>	<input type="text" value="wp_"/>	Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.
<input type="button" value="Enviar"/>		

Para ponérselo más complicado, es recomendable no hacer uso del prefijo por defecto y utilizar letras y números aleatorios. Por ejemplo **“sy45x\_”**.

En el caso de que ya tengamos realizada la instalación, podemos modificar sin problema. Para ello, deberemos editar el archivo **“wp-config.php”** y cambiar el valor asociado a la variable **“\$table\_prefix”**.

## PHP

```
$table_prefix = 'sy45x_';
```

Además de este cambio, también es necesario modificar el nombre de todas y cada una de las tablas que forman parte de la base de datos. Para ello, desde el **phpMyAdmin** deberíamos ejecutar las siguientes sentencias SQL, una por cada tabla que tengamos en nuestra base de datos.

## SQL

```
RENAME TABLE wp_links TO sy45x_links;
```

Por último, faltaría buscar en las tablas **“sy45x\_options”** y **“sy45x\_usermeta”** registros que contengan referencias al anterior prefijo **“wp\_”**. Esto lo podemos hacer con las siguientes instrucciones SQL

## SQL

```
SELECT * FROM sy45x_options WHERE option_name LIKE '%wp_%';  
SELECT * FROM sy45x_usermeta WHERE meta_key LIKE '%wp_%';
```

Por cada resultado, habría que realizar un Update.

## SQL

```
UPDATE sy45x_options SET option_name = '1a2b3c_user_roles' WHERE option_name = 'wp_user_roles';
```

## No utilizar el usuario admin

Otra de las acciones que mejoran la seguridad de WordPress es no hacer uso del usuario admin. Este usuario, si no se indica lo contrario, se crea por defecto durante la instalación. Si estamos instalando desde cero WordPress, podremos indicar un usuario diferente al admin, ya que éste será el primero que probará un hacker para tomar el control de tu web. Por ejemplo, en la imagen que os dejamos a continuación hemos indicado “berto”.

### Hola

---

¡Bienvenido al famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo.

### Información necesaria

---

Por favor, debes facilitarnos los siguientes datos. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

**Título del sitio**

**Nombre de usuario**

Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

**Contraseña**

**Fuerte**

**Importante:** Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

En el caso de que ya lo tengamos creado, lo recomendable es eliminarlo desde la gestión de usuarios de WordPress. Para ello, será necesario que exista al menos otro usuario con rol de administrador.

Tampoco debemos olvidarnos de las **contraseñas** asignadas a los usuarios. Estas deben ser lo más complejas posibles para evitar problemas de seguridad.

## Proteger el archivo de configuración de WordPress

El archivo de configuración de WordPress, el fichero **“wp-config.php”**, contiene información muy sensible sobre el servidor y la configuración del CMS. Para mejorar su seguridad, y evitar que puedan acceder a su contenido, se pueden tomar ciertas medidas.

La primera de ellas es cambiar los permisos del archivo para protegerlos contra escritura. Podemos asignarles permisos 444 o 440. Además de esto, también es recomendable bloquear los accesos no deseados. Esto dependerá del servidor que estemos utilizando.

En el caso de ser Apache, en el archivo **.htaccess** deberíamos añadir las siguientes líneas.

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

Si por el contrario, el servidor web utiliza Nginx, las líneas que deberíamos utilizar para bloquear el acceso serían las siguientes.

```
location /wp-config.php {  
    deny all;  
}
```

## Proteger la carpeta de archivos subidos

La carpeta “**uploads**”, ubicada dentro de “**wp-content**” de la instalación de WordPress, es donde se suben todos los archivos desde el administrador del CMS. Este directorio es el más susceptible de sufrir ataques, de modo que es muy importante protegerlas para evitar que se ejecuten desde su interior scripts maliciosos.

Aunque WordPress, por defecto, no permite la subida de archivos ejecutables en el interior de esta carpeta, los hackers utilizan ciertas técnicas para saltarse esta protección. Para garantizar la seguridad, debemos aplicar una protección extra, definiendo expresamente el tipo de extensiones de los archivos que se podrán subir. Al igual que en el punto anterior, tenemos dos opciones, según utilicemos Apache o Nginx.

En el caso de Apache, las líneas a añadir en el fichero .htaccess serían las siguientes:

```
<Files ~ ".*\..*">  
    Order Allow,Deny  
    Deny from all  
</Files>  
<FilesMatch "\.(jpg|jpeg|jpe|gif|png|bmp|tif|tiff|doc|pdf|rtf|xls)$">  
    Order Deny,Allow  
    Allow from all  
</FilesMatch>
```

En el caso de Nginx, en su archivo de configuración añadiríamos lo siguiente:

```
location ~ .*\..* {  
    deny all;  
}  
  
location ~ \.(jpg|jpeg|jpe|gif|png|bmp|tif|tiff|doc|pdf|rtf|xls)$ {  
    allow all;  
}
```

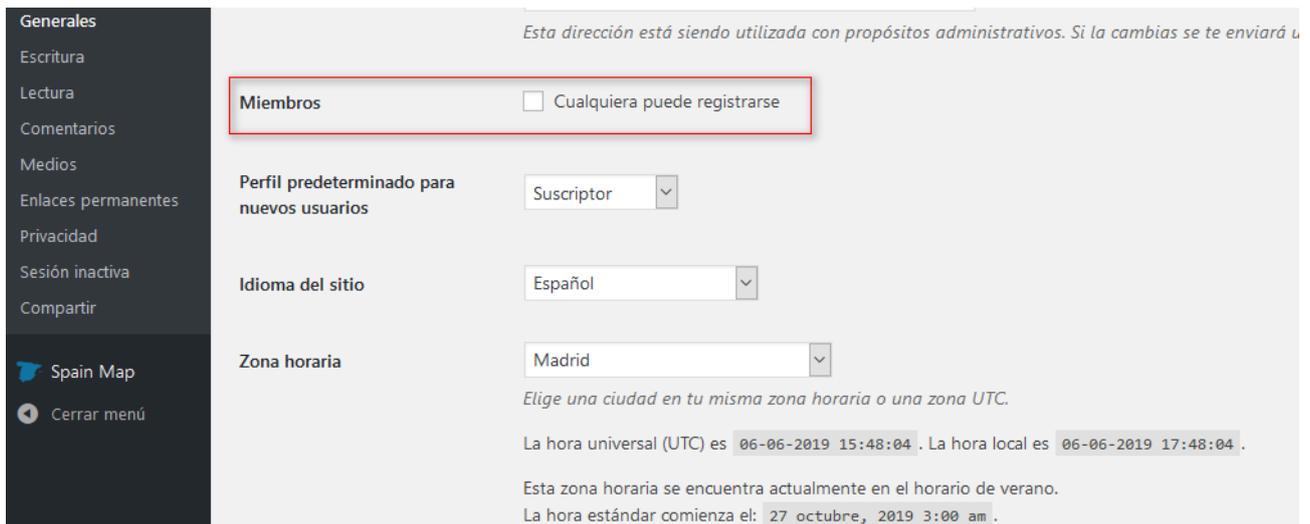
En nuestro ejemplo hemos indicado algunas extensiones, pero podrían ser más o menos, según nuestras necesidades.

## Limita los intentos de login

Una de las principales formas de atacar WordPress es hacerlo mediante el sistema de fuerza bruta. Este ataque consiste en ir probando miles de usuarios y contraseñas en tu login hasta dar con una correcta. Sin embargo, es posible evitar este tipo de ataques de forma muy sencilla y es limitando el número de intentos para loguearse. Si se alcanza ese número de intentos erróneos, el acceso se bloquearía durante un determinado tiempo.

Para añadir esta limitación, podemos utilizar varios plugins aunque **Loginizer** puede funcionar bastante bien. La idea es configurarlo con un número bajo de intentos pero que te deje maniobrar por si nos equivocamos. Un valor entre tres y cinco podría ser adecuado.

Dentro de este apartado, también sería recomendable inhabilitar el registro de usuarios para evitar que usuarios con malas intenciones aprovechen alguna vulnerabilidad para obtener permisos extras. Para desactivar esta opción debemos hacerlo desde la opción "**Generales**" que está dentro de "**Ajustes**" en el menú de la administración.



Esta dirección está siendo utilizada con propósitos administrativos. Si la cambias se te enviará u

**Miembros**  Cualquiera puede registrarse

Perfil predeterminado para nuevos usuarios: Suscriptor

Idioma del sitio: Español

Zona horaria: Madrid

Elige una ciudad en tu misma zona horaria o una zona UTC.

La hora universal (UTC) es 06-06-2019 15:48:04 . La hora local es 06-06-2019 17:48:04 .

Esta zona horaria se encuentra actualmente en el horario de verano.

La hora estándar comienza el: 27 octubre, 2019 3:00 am .

Por último, en lo que al apartado de login se refiere, no olvidéis añadir algún sistema de comprobación humana como reCaptcha que evite accesos indeseados de máquinas automáticas. Hay mucho plugins para ello, por ejemplo [Login No Captcha reCAPTCHA](#).

## Instala un plugin de seguridad

En el repositorio de plugins de WordPress podemos encontrarnos plugins especializados en proteger WordPress. La mayoría de ellos contienen ajustes que evitan ataques por fuerza bruta, inyección de código o modificaciones de archivos, incluyendo sistemas de avisos ante cualquier posible ataque. [WordFence](#) y [iThemes Security](#) son dos de estos plugins.

# Deshabilitar XML-RPC

WordPress incluye en su core el archivo “**xmlrpc.php**” que ofrece ciertas funcionalidades al CMS como puede ser la posibilidad de conectar la aplicación WordPress para iOS o Android, el uso de editores offline o algunos sistemas de sindicación de contenidos. El problema es que este archivo también deja abierta una vía de posibles ataques. En el caso de que tenga muy claro que nunca utilizarás estas funcionalidades, lo más recomendable es que bloqueases el acceso. Veamos con hacer esto tanto en Apache como en Nginx.

En el servidor Apache se añadiría las siguientes líneas en el archivo .htaccess.

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

Si se utilizase Nginx, el código que habría que añadir sería el siguiente.

```
location /xmlrpc.php {  
    deny all;  
}
```

# Esconder la versión de WordPress

```

30 }
31 </style>
32 <link rel='stylesheet' id='twentyineteen-jetpack-css' href='https://c0.wp.com/p/jetpack/7.2.1/modules/theme-tools/co
33 <link rel='stylesheet' id='wp-block-library-css' href='https://c0.wp.com/c/5.1.1/wp-includes/css/dist/block-library/style
34 <link rel='stylesheet' id='wp-block-library-theme-css' href='https://c0.wp.com/c/5.1.1/wp-includes/css/dist/block-library
35 <link rel='stylesheet' id='twentyineteen-style-css' href='http://wptest.icolorvivo.com/wp-content/themes/twentyineteen/
36 <link rel='stylesheet' id='twentyineteen-print-style-css' href='http://wptest.icolorvivo.com/wp-content/themes/twentyin
37 <link rel='stylesheet' id='jetpack-css-css' href='https://c0.wp.com/p/jetpack/7.2.1/css/jetpack.css' type='text/css' medi
38 <script type='text/javascript' src='https://c0.wp.com/c/5.1.1/wp-includes/js/jquery/jquery.js'></script>
39 <script type='text/javascript' src='https://c0.wp.com/c/5.1.1/wp-includes/js/jquery/jquery-migrate.min.js'></script>
40 <link rel='https://api.w.org/' href='http://wptest.icolorvivo.com/wp-json/' />
41 <link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://wptest.icolorvivo.com/xmlrpc.php?rsd" />
42 <link rel="wlymanifest" type="application/wlymanifest+xml" href="http://wptest.icolorvivo.com/wp-includes/wlymanifest.xml"
43 <meta name="generator" content="WordPress 5.1.1" />
44 <link rel="snortlink" href="https://wp.me/avzBd" />
45
46 <link rel='dns-prefetch' href='//v0.wordpress.com/'/>
47 <link rel='dns-prefetch' href='//c0.wp.com/'/>
48 <link rel='dns-prefetch' href='//10.wp.com/'/>
49 <link rel='dns-prefetch' href='//11.wp.com/'/>
50 <link rel='dns-prefetch' href='//12.wp.com/'/>
51 <style type='text/css'>img#wpstats{display:none}</style> <style type="text/css">.recentcomments a{display:inline !i
52 <style type="text/css">
53

```

Conocer la versión que utiliza un sitio web desarrollado con WordPress puede ser de gran ayuda para los atacantes, ya que si se trata de una versión antigua, podría tener vulnerabilidades conocidas por ellos para esa determinada versión. Debido a esto, es recomendable esconder la versión que utiliza la instalación. Para ello, en el archivo **“functions.php”** del tema que estemos utilizando, deberíamos añadir el siguiente código PHP.

## PHP

```

function wp_version_remove_version() {
    return "";
}
add_filter('the_generator', 'wp_version_remove_version');

```

De esta forma, la versión utilizada ya no se mostrará en el encabezado del código.

# Desactivar la opción de edición de archivos desde la administración

WordPress da la opción de editar los archivos del tema desde su administración, algo que puede suponer un importante problema si alguien consigue acceder a nuestro sitio. Para evitar que se modifique el código sin nuestro consentimiento, es muy buena práctica desactivar la opción de editar archivos desde la administración. Para conseguir esto, bastaría con añadir la siguiente línea dentro del archivo **"wp-config.php"** de nuestra instalación.

## PHP

```
define('DISALLOW_FILE_EDIT', true);
```

Como hemos podido ver a lo largo de nuestro [White Paper](#), hay numerosas maneras de mejorar la seguridad de la instalación de nuestro WordPress. Ya depende de cada uno aplicar aquellas que considere más oportunas para él.