

Webinar

# La seguridad en WordPress empieza en mí

Tomás Sierra Campos

# Tomás Sierra

Profesor-tutor de Sistemas Microinformáticos y Redes en el CFP López Vicuña de Santander.

Soy maestro, formador y formador online, desarrollador web frontend y backend especializado en ciberseguridad y WordPress.

Intento formar a padres, madres, adolescentes y profesores en usos seguros de internet.

Más de 4000 horas de formación en Congresos, cursos y talleres.

Organizador del congreso de Ciberseguridad Sh3llcon y de la WordCamp Santander



# Lo primero de todo...

# Utiliza un buen hosting

- Optimizado para WordPress.
- Buenas políticas de seguridad a nivel de servidor.
- Avisos de actualizaciones.

# Parámetros esenciales de seguridad

- Backup preventivo
- Actualización de plugins y plantilla del tema.
- Modificar prefijos de la base de datos.
- Modificar permisos en archivos y directorios.
- Fortificar archivos críticos.
- Indexar directorios para impedir listado de archivos.
- Deshabilitar el editor de archivos del BackEnd.
- Deshabilitar y desinstalar plugins inactivos.

# Parámetros esenciales de seguridad

- Instalar plugin de seguridad y realizar escaneo de archivos en busca de código malicioso.
- Modificar el ID del usuario administrador
- Modificar el nombre y alias del usuario administrador
- Modificar las claves SALT
- Configurar parámetros de .htaccess para restringir el acceso a archivos desde url.
- Cambiar la ruta de acceso al panel de control "wp-admin"
- Backup de datos.

# Qué debe tener (como mínimo) un plugin seguridad de WordPress

- Modificar ruta al panel de control: /wp-admin/
- Limita intentos de acceso
- Modificar prefijo tablas
- No usar usuario "admin"
- WAF (Web Application Firewall)
- Escaneo de archivos
- Configura permisos de archivos
- Obligar contraseñas fuertes

## Modificar la ruta de acceso al panel de control

[miweb.com/wp-admin](https://miweb.com/wp-admin)

[miweb.com/paneldegestion](https://miweb.com/paneldegestion)





Modifica ruta al panel de control: /wp-admin/

### Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

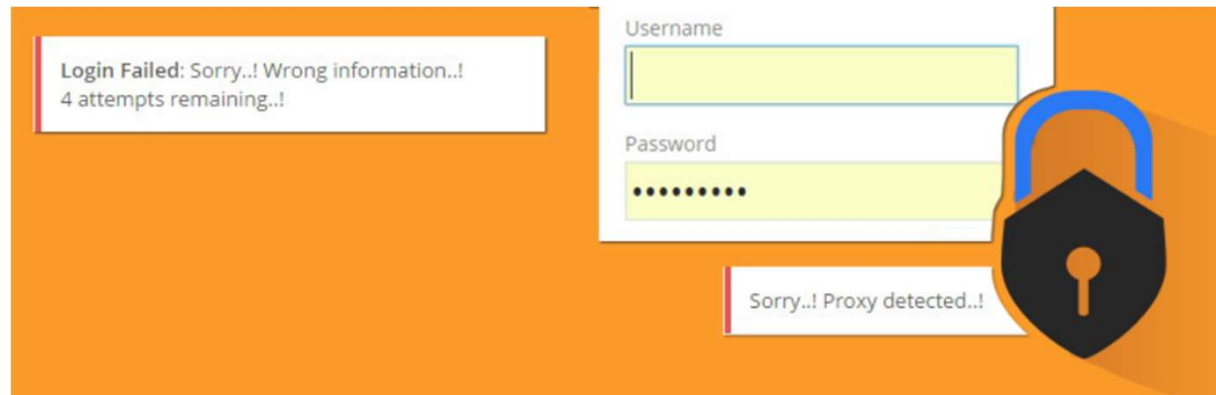
WAF (Web Application Firewall)

Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## Limitar el número de intentos de acceso al panel de control.



**Plugins:**

**Limit login attemps...**

**Wordfence, Sucuri, All In One WP Security & Firewall...**

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

**Modificar prefijo tablas**

No usar usuario "admin"

WAF (Web Application Firewall)

Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## Modificar prefijos de la bbdd

Modificar el prefijo por defecto **wp\_**  
por algo como **lsdjdujm\_**

### Plugins como:

Sucuri  
All in 1 WP Security and Firewall  
Ithemes Security...

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

**No usar usuario "admin"**

WAF (Web Application Firewall)

Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## No usar usuario “admin”



The image shows the WordPress login interface. At the top center is the WordPress logo. Below it is a white login box with a light gray border. Inside the box, the text "Nombre de usuario o dirección de correo electrónico" is above a text input field. The word "admin" is typed into this field, with a red squiggly underline underneath it. Below the first field is the text "Contraseña" above another text input field. At the bottom left of the box is a checkbox labeled "Recuérdame". At the bottom right is a blue button with the text "Acceder" in white.

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

**Modificar la ID del usuario administrador**

WAF (Web Application Firewall)

Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## Modificar la ID del usuario administrador

mipaginaweb.es/?autor=1

mipaginaweb.es/author/admin/



Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

Modificar la ID del usuario administrador

**WAF (Web Application Firewall)**

Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## WAF (Web Application Firewall)

Protege sus aplicaciones web filtrando, vigilando y bloqueando todo el tráfico HTTP/S malicioso que se dirija hacia ellas e impide que salga de ellas cualquier dato no autorizado.

Lo hace a través de un conjunto de políticas que distinguen entre tráfico malicioso y seguro.

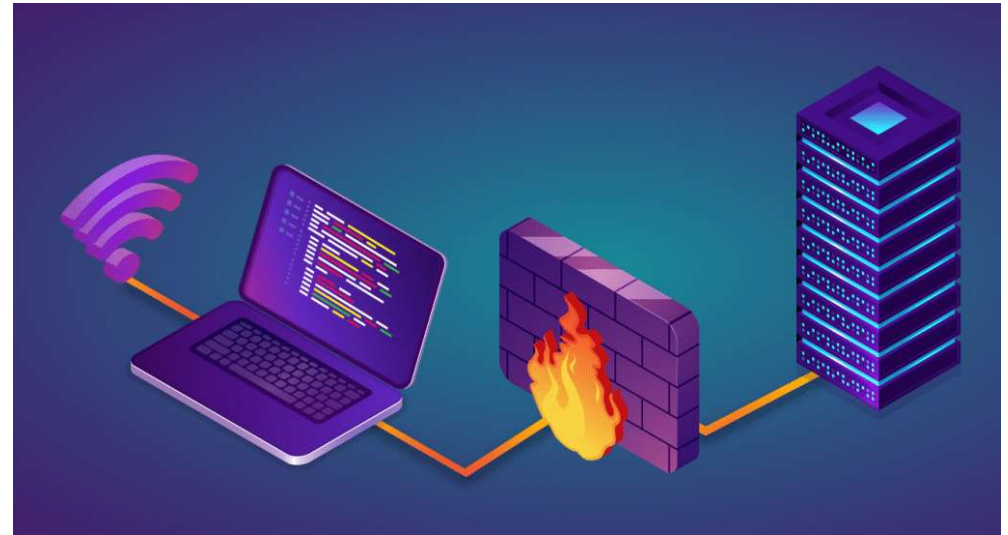


Imagen: logix.in

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

Modificar la ID del usuario administrador

WAF (Web Application Firewall)

### Escaneo de archivos

Configura permisos de archivos

Obligar contraseñas fuertes

## Escaneo de archivos

Scan Settings Settings Saved! Quick Scan: WP\_Core Plugins Themes

### Complete Scan Status

Scanning .../public\_html/wp-admin/css

2 Folders Checked  
33 Seconds Elapsed

1%

144 Folders Remaining  
36 Minutes Remaining

0 Archivos en Cuarentena

Found 0 htaccess Threats

Found 0 TimThumb Exploits

Found 0 Backdoor Scripts

Found 0 Known Threats

Found 0 Core File Changes

Found 0 Potential Threats

Pause

103 Archivos Escaneados

146 Carpetas Seleccionadas

2 Carpetas Escaneadas

0 Carpetas Omitidas

1 Archivos Omitido

0 Errores de Lectura/Escritura

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

Modificar la ID del usuario administrador

WAF (Web Application Firewall)

Escaneo de archivos

**Configura permisos de archivos**

Obligar contraseñas fuertes

## Configurar permisos de archivos

### Archivos: 644 (RW / R / R)

El propietario puede **leer** y **escribir** en el archivo

Los demás solo pueden **leer**.

### Carpetas: 755 (RWX / RW / RW)

El propietario del archivo puede **leer, escribir y ejecutar** en el archivo.

Los demás usuarios pueden **leer y escribir** en el archivo pero no ejecutar.

Modifica ruta al panel de control: /wp-admin/

Limita intentos de acceso

Modificar prefijo tablas

No usar usuario "admin"

Modificar la ID del usuario administrador

WAF (Web Application Firewall)

Escaneo de archivos

Configura permisos de archivos

**Obligar contraseñas fuertes**

## Obligar contraseñas fuertes

### ¿Qué es una contraseña fuerte?

1. Que no aparezca en un diccionario
2. Que solo yo la recuerde.
3. Que tenga como mínimo 12 caracteres.
4. Que contenga letras mayúsculas y minúsculas
5. Que contenga números
6. Que contenga símbolos

# NO

123456



admin



# SI

\*NhmqpbnV\_13579

4gR570\$CF5&amp;I



## Obligar contraseñas fuertes

Servicios online para crear contraseñas fuertes

<https://www.clavesegura.org/es/>

<https://password-generate.com/es/>

<https://www.eset.com/es/password-generator/>

<https://www.lastpass.com/es/features/password-generator>



The image shows the ClaveSegura password generator interface. At the top, there is a logo with a padlock icon and the text "ClaveSegura" and "Generador de contraseñas seguras bajo SSL". Below this, a large grey box displays the generated password "qa:bv1+2@dM1". Underneath the password box is a pink button with a key icon and the text "Generar nueva contraseña". To the right of the button is a "Nivel de seguridad:" label and a green progress bar. Below the button and progress bar are two settings boxes. The "Tipo" box has the label "Elige el tipo de clave a generar:" and a dropdown menu showing "Todos los caracteres". The "Longitud" box has the label "Selecciona el nº de caracteres:" and a dropdown menu showing "12".

 **ClaveSegura**  
Generador de contraseñas seguras bajo SSL

qa:bv1+2@dM1

 Generar nueva contraseña

Nivel de seguridad: 

**Tipo**  
Elige el tipo de clave a generar:  
Todos los caracteres ▼

**Longitud**  
Selecciona el nº de caracteres:  
12 ▼

## Obligar contraseñas fuertes

Servicios online para comprobar la fortaleza de tus contraseñas

<https://password.es/comprobador/>

<https://es.vpnmentor.com/herramientas/passwordmeter/>

<https://password.kaspersky.com>

**Comprobador de Contraseñas/Password**

[Inicio](#) | [Email Marketing](#) | [Juegos](#) | [test de velocidad adsl](#)

### Curso de Control Numérico

Formación 100% Online: 150 Horas 6 ECTS. Titulación UCAV Online seas.es

Change language: [castellano](#) | [english](#) | [italiano](#) | [aleman](#) | [catalan](#) | [frances](#) | [portugues](#)

| Prueba tu Contraseña |  | Requerimientos mínimos   |
|----------------------|--|--|
| Contraseña:          | <input type="password" value="*****"/> | <ul style="list-style-type: none"><li>• Tamaño mínimo de 8 caracteres</li><li>• Contener al menos 3-4 de las siguientes cosas:<ul style="list-style-type: none"><li>- Letras en Mayúsculas</li><li>- Letras en Minúsculas</li><li>- Números</li><li>- Símbolos</li></ul></li></ul> |
| Ocultar:             | <input checked="" type="checkbox"/>    |  |
| Resultado:           | <div><div>100%</div></div>             |  |
| Complejidad:         | Very Strong                            |  |



## Wordfence



+4.000.000 Descargas

Configuración **nivel Medio**.

Ajustes básicos a 1 clic

Permite Exportar / Importar configuración

NO Permite actualizaciones automáticas

modifica ruta /wp-admin/

Limita intentos de acceso

Modifica prefijo tablas

WAF (cortafuegos de aplicaciones web)

Escaneo de archivos

DESHABILITAR archivo xmlrpc.php

NO Desconecta usuario tras inactividad

Cambiar Permisos de archivos críticos

Desactivar la edición de archivos desde WordPress

Live Traffic

Copias de seguridad

Cambio de claves SALT

## Modificar las claves SALT en wp-config.php

```
define('AUTH_KEY',                'pco,vDP>n8Ygho9Y0}Ad0U$w|ggXaTq8|y:@;:=ot-_Edej>1Xh-x>BXpGq+#F!l');
define('SECURE_AUTH_KEY',        '&)(>miFL17ktv#m*=a+%Sq|E$~V5q/e3q<2C~Yj[D.UXk,DkY1~KPA+$ZT2v<_Y6');
define('LOGGED_IN_KEY',          'wOEBNyU]~KF:`3Y3LoG rN=6Z^HqZb0RDhLP9^|oJQv>.)o$wTm356=riA.0ULNk');
define('NONCE_KEY',              '5AWgGE,5{2c0zQ@oySUyjQuz8snL7rx8 wPd}=%1w09Y-&tviw&!j]yKoq|5b@e0');
define('AUTH_SALT',              '{hgF+x(j l:-CjC*S<]5.-{*nPjn?|pU`f`K/+vn+|40zL[g=F9+T]g#ocS6h.a$');
define('SECURE_AUTH_SALT',       '$RHre}-9pfB1J61yb7|v%>OGL~rat-Jj@d@=JSt}t-[/<$Y(i1QPc:#!Y[x57l<');
define('LOGGED_IN_SALT',         'F?6%3+X1B$U#g<j~l2M9Hbu,9 )Q91?^n9t&Eh3lFL#Kl{jY|*w~|Z!`e`Ad|800');
define('NONCE_SALT',             '+zZ+k!@`hYy~EfKmF[ndERZN+LMrvZ6|_gBw0:|l=z_PC2!qn+6Md{+}@8YRXa[^');
```

## iThemes Security



+1.000.000 Descargas

Configuración **nivel Medio**.

Ajustes básicos a 1 clic

NO Permite Exportar / Importar configuración

NO Permite actualizaciones automáticas

modifica ruta /wp-admin/

Limita intentos de acceso

Modifica prefijo tablas

WAF (cortafuegos de aplicaciones web)

Escaneo de archivos

DESHABILITAR archivo xmlrpc.php

NO Desconecta usuario tras inactividad

Cambiar Permisos de archivos críticos

Desactivar la edición de archivos desde WordPress

Live Traffic

Copias de seguridad de Base de Datos

Cambio de claves SALT

## All In One WP Security & Firewall



+1.000.000 Descargas

Configuración nivel **fácil** pero **larga**.  
(Sistema de puntos)

Permite Exportar / Importar configuración

NO Permite actualizaciones automáticas

modifica ruta /wp-admin/

Limita intentos de acceso

Modifica prefijo tablas

WAF (cortafuegos de aplicaciones web)

Escaneo de archivos

DESHABILITAR archivo xmlrpc.php

NO Desconecta user tras inactividad

Cambiar Permisos de archivos críticos

Desactivar la edición de archivos desde WordPress

Live Traffic

Copias de seguridad de *.htaccess* y *wp-config.php*

Cambio de claves SALT

## Sucuri



+800.000 Descargas

Configuración **Larga** y algo tediosa.  
ajustes básicos a 1 clic

NO Permite Exportar / Importar configuración

NO Permite actualizaciones automáticas

modifica ruta /wp-admin/

Limita intentos de acceso

Modifica prefijo tablas

WAF (cortafuegos de aplicaciones web)

Escaneo de archivos

DESHABILITAR archivo xmlrpc.php

NO Desconecta user tras inactividad

Cambiar Permisos de archivos críticos

Desactivar la edición de archivos desde WordPress

Live Traffic

NO Copias de seguridad

Cambio de claves SALT



|   | Wordfence  | iThemes Security                      | All in One WP Security & Firewall       | Sucuri          |
|---|------------|---------------------------------------|---|-----------------|
| Descargas   | >4.000.000 | >1.000.000                            | >1.000.000                              | >800.000        |
| Configuración                                     | Media      | Media.<br>ajustes básicos<br>a 1 clic | Fácil pero larga<br>(Sistema de PUNTOS) | Larga y tediosa |
| Exportar / Importar configuración                 | SI         |                                       | SI                                      |                 |
| Permite actualizaciones automáticas               |            |                                       |   |                 |
| modifica ruta /wp-admin/                          | ---        | SI                                    | SI                                      | SI              |
| Limita intentos de acceso                         | SI         | SI                                    | SI                                      | SI              |
| Modifica prefijo tablas                           |            | SI                                    | SI                                      | SI              |
| WAF   | SI         |                                       | SI                                      | SI (de pago)    |
| Escaneo de archivos                               | SI         | SI                                    | SI                                      | SI              |
| DESHABILITAR xmlrpc.php                           |            | SI                                    | SI                                      | SI              |
| Desconecta user tras xx minutos de inactividad    |            |                                       |   |                 |
| Permisos de archivos críticos                     |            | SI                                    | SI                                      |                 |
| Desactivar la edición de archivos desde WordPress |            |                                       |   |                 |
| Live Traffic                                      | SI         |                                       |   | SI              |
| Copias de seguridad                               |            | Base de datos                         | .htaccess<br>wp-config.php              |                 |
| CAMBIO DE SALTS                                   |            | SI                                    |   | SI              |



Webinar: La seguridad en WordPress empieza en mí 



|   | Wordfence  | iThemes Security                      | All in One WP Security & Firewall       | Sucuri          | Shield Security  |
|---|------------|---------------------------------------|---|-----------------|------------------|
| Descargas   | >1.000.000 | >800.000                              | >500.000                                | >300.000        | >50.000          |
| Configuración                                     | Media      | Media.<br>ajustes básicos<br>a 1 clic | Fácil pero larga<br>(Sistema de PUNTOS) | Larga y tediosa | Fácil pero larga |
| Exportar / Importar configuración                 | SI         |                                       | SI                                      |                 |                  |
| Permite actualizaciones automáticas               |            |                                       |   |                 | SI               |
| modifica ruta /wp-admin/                          |            | SI                                    | SI                                      | SI              | SI               |
| Limita intentos de acceso                         | SI         | SI                                    | SI                                      | SI              | SI               |
| Modifica prefijo tablas                           |            | SI                                    | SI                                      | SI              |                  |
| Firewall  | SI         |                                       | SI                                      | SI (de pago)    | SI               |
| Escaneo de archivos                               | SI         | SI                                    | SI                                      | SI              | Sólo del Core    |
| DESHABILITAR xmlrpc.php                           |            | SI                                    | SI                                      | SI              | SI               |
| Desconecta user tras xx minutos de inactividad    |            |                                       | SI                                      |                 | SI               |
| Permisos de archivos críticos                     |            | SI                                    | SI                                      |                 |                  |
| Desactivar la edición de archivos desde WordPress |            |                                       |   |                 | SI               |
| Live Traffic                                      | SI         |                                       |   | SI              | SI               |
| Copias de seguridad                               |            | BBDD                                  | .htaccess<br>wp-config.php              |                 |                  |
| CAMBIO DE SALTS                                   |            | SI                                    |   | SI              |                  |

¡Muy bien!

Entonces la pregunta es...



# MUCHAS GRACIAS



[www.tomassierra.com](http://www.tomassierra.com)



[@Tomycant](https://twitter.com/Tomycant)



<https://www.facebook.com/tomycant>