# Asegura tu WordPress

## ¿Qué voy a explicar?

1. Las cosas básicas que todo el mundo ha explicado ya
2. Las cosas básicas que la gente explica pero no hace (y me incluyo)
3. Las cosas no tan básicas, pero que habría que hacerse
4. Las cosas que realmente hacen que tu WordPress sea seguro

# Asegura tu WordPress

## Las cosas básicas que todo el mundo ha explicado ya

- Hosting decente

- Mantener al día WordPress (core, plugins y themes)

- Eliminar luser: "`admin`" / "`1`"

- Prefijo de tablas ≠ "`wp_`"
Ya puestos, usar una combinación extraña, tipo "a1b2c3_" de al menos 6 caracteres [a-zA-Z0-9]

- Siempre usar certificado TLS SHA-256 (Let's Encrypt) y forzar su uso

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

# Asegura tu WordPress

## Las cosas básicas que todo el mundo ha explicado ya

- Desde la versión 2.6, usar las "Security Keys" (los caracteres raros del `wp-config`)

```
define('AUTH_KEY',         't`DK%X:>xy|e-Z(BXb/f(Ur`8#~Uz');
define('SECURE_AUTH_KEY',  'D&ovlU#|CvJ##uNq}bel+^MFtT&.b');
define('LOGGED_IN_KEY',    'MGKi8Br(&{H*~&0s;{k0<S(O:+f#W');
define('NONCE_KEY',        'FIsAsXJKL5ZlQo)iD-pt??eUbdc{_');
define('AUTH_SALT',        '7T-!^i!0,w)L#JK@pc2{8XE[DenYI');
define('SECURE_AUTH_SALT', 'I6`V|mDZq21-J|ihb u^q0F }F_NU');
define('LOGGED_IN_SALT',   'w<$4c$Hmd%/*]`Oom>(hdXW|0M=Xa');
define('NONCE_SALT',       'a|#h{c5|P &xWs4IZ20c2&%4!c(/x');
```

# Asegura tu WordPress

## Las cosas básicas que todo el mundo ha explicado ya

- Activar la caché, "*ofcors*"

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

- Que WordPress se actualice sólo

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

- Activar un AntiSpam, como Akismet

Akismet Anti-Spam
https://wordpress.org/plugins/akismet/

# Asegura tu WordPress

## Las cosas básicas que la gente explica pero no hace

- Fijar la URL de la web en el fichero de configuración
(que la gente es muy manazas y toca en el panel!)

```
define('WP_SITEURL',     'https://www.example.com');
define('WP_HOME',        'https://www.example.com');
```

- Cambiar las carpetas por defecto (de uploads, plugins, etc...)

```
define('WP_CONTENT_DIR', '/mis-contenidos-aqui');
define('WP_CONTENT_URL', 'https://www.example/mi-content-aqui');
define('WP_PLUGIN_DIR',  '/mis-contenidos-aqui/cosicas');
define('WP_PLUGIN_URL',  'https://www.example/mi-content-aqui/cosicas');
define('UPLOADS',        'mi-content-aqui/mis-fichericos’);
$theme_root =           WP_CONTENT_DIR.'/como-se-ve-la-cosa';
```

# Asegura tu WordPress

## Las cosas básicas que la gente explica pero no hace

- La cookie de Administración, sólo para Administración.

```
define('ADMIN_COOKIE_PATH', 'https://www.example/wp-admin');
```

- Permisos de los ficheros.

Que siempre se dice de usar 755 en carpetas y 644 en ficheros.

- Carpetas: 750
- Ficheros: 640
- wp-config.php: 600

- Impedir la lectura del readme.html

Ya sea eliminando el fichero, impidiendo su acceso… incluye la versión de WordPress.

# Asegura tu WordPress

## Las cosas básicas que la gente explica pero no hace

- Desactivar la edición de ficheros desde el panel

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

- Incluso, que nadie pueda instalar plugins / temas

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

# Asegura tu WordPress

## Las cosas básicas que la gente explica pero no hace

- Bloquear peticiones externas

pero que WordPress se pueda actualizar, al menos

```
define('WP_HTTP_BLOCK_EXTERNAL', true);
define('WP_ACCESSIBLE_HOSTS', '*.wordpress.org,*.github.com');
```

- Mantener un poco de limpieza en la subida de imágenes (y las generadas)

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

# Asegura tu WordPress

## Las cosas no tan básicas, pero que habría que hacer

- Bloquear funcionamiento de PHP en carpetas tipo `/uploads/`

Normalmente se hace por el servidor web, diciéndole que en determinadas carpetas el PHP no se ejecute (obviamente hay que saber un poco de sistemas para hacer esto)

- El acceso a la base de datos sólo desde la misma máquina (localhost / firewall cerrado) o sólo la IP de la máquina web (y la local).

- Eliminar cabeceras que no convienen (como la versión de WordPress y otras)

`EliminaCabeceras`

http://bit.ly/EliminaCabeceras

Este es un pequeño plugin mío, personal y transferible, que podría ser un functions.php en tu plantilla...

# Asegura tu WordPress

## Las cosas no tan básicas, pero que habría que hacer

- Bloquear "cosas raras" (ataques, etc...) a modo Firewall

`Wordfence Security`
https://wordpress.org/plugins/wordfence/

Muy interesante la sección "Live Traffic".

- Hacer Backups / Copias de Seguridad (¿obvio?)

`BackWPup`
https://wordpress.org/plugins/backwpup/

# Asegura tu WordPress

## Las cosas no tan básicas, pero que habría que hacer

- Analizar el propio sistema de ficheros, malware, etcétera.

Sucuri Security – Auditing, Malware Scanner and Security Hardening
https://wordpress.org/plugins/sucuri-scanner/

· Security Activity Audit Logging
· File Integrity Monitoring
· Remote Malware Scanning
· Blacklist Monitoring
· Effective Security Hardening
· Post-Hack Security Actions
· Security Notifications

# Asegura tu WordPress

## Las cosas que realmente hacen que tu WordPress sea seguro

- Asegurar **el sistema**:

Esto básicamente se resumen en:

· Hacer las cosas bien (léase, todo lo que ya se ha explicado)

· Sentido Común (seguramente esto es más difícil que todo lo anterior)

# Asegura tu WordPress

## Las cosas que realmente hacen que tu WordPress sea seguro

- Asegurar los **usuarios torpes**:

Los lusers suelen hacer tonterías, por eso es importante que:

- No puedan tocar mucho, pero que crean que sí.
- **Oblígales** a usar un sistema 2FA (Second-Factor Authentication)

2FAS Light - Google Authenticator
https://wordpress.org/plugins/2fas-light/

Latch
https://wordpress.org/plugins/latch/

**"Si todo el mundo utilizase 2FA, Internet sería muchísimo más seguro."**

# Asegura tu WordPress

## Bonus Track

Habitualmente hay 2 tipos de inyección de código malicioso:

- Añadir código a la plantilla del WordPress

Habitualmente para mostrar enlaces o contenido con una serie de reglas que hacen que tú no suelas verlos.

- Introducir ficheros en el sistema

Suelen utilizarse para que tu instalación esté dentro de un conjunto de máquinas fantasma, y poder hacer ataques a otros sistemas.

# Asegura tu WordPress

## Bonus Track

**WordPress es seguro**, los seres humanos un poco menos.

Una instalación “core” de WordPress con una configuración básica de base es lo suficientemente segura para sólo preocuparse de tenerlo actualizado y publicar.

En el momento en el que instalas plugins o plantillas de sitios “poco fiables”, o que hacen “inventos raros” es *cuando empieza la fiesta*.