Seguridad en WordPress con presupuesto cero



Meetup WordPress Coruña

Fernando Tellado · AyudaWP.com · @fernandot

Seguridad para pobres en tres actos

RUTA

1

Lo que WordPress ya hace bien

Defensas de serie y ajustes del escritorio. Sin plugins ni código.

2

Lo que hace mal o le falta

El arreglo en tres sitios: wp-config.php, .htaccess y un archivo PHP.

3

Vigilante, para comprobarlo

La revisión de todo lo anterior y lo que el código no alcanza.

ACTO 1

Lo que WordPress ya hace bien

Sin plugins ni nada



Lo que viene de serie y no se ve

ACTO 1

Contraseñas con bcrypt

Desde WordPress 6.8, mucho más difíciles de reventar

Nonces en cada acción

Otra web no puede hacerte pulsar un botón de tu escritorio

Cookies HttpOnly

Un script inyectado no puede leer tu sesión

Subidas filtradas

La biblioteca de medios rechaza PHP y ejecutables

Recuperación con caducidad

Los enlaces de restablecer claves duran 24 horas

Actualizaciones de seguridad solas

Las menores del núcleo se actualizan desde WP 3.7

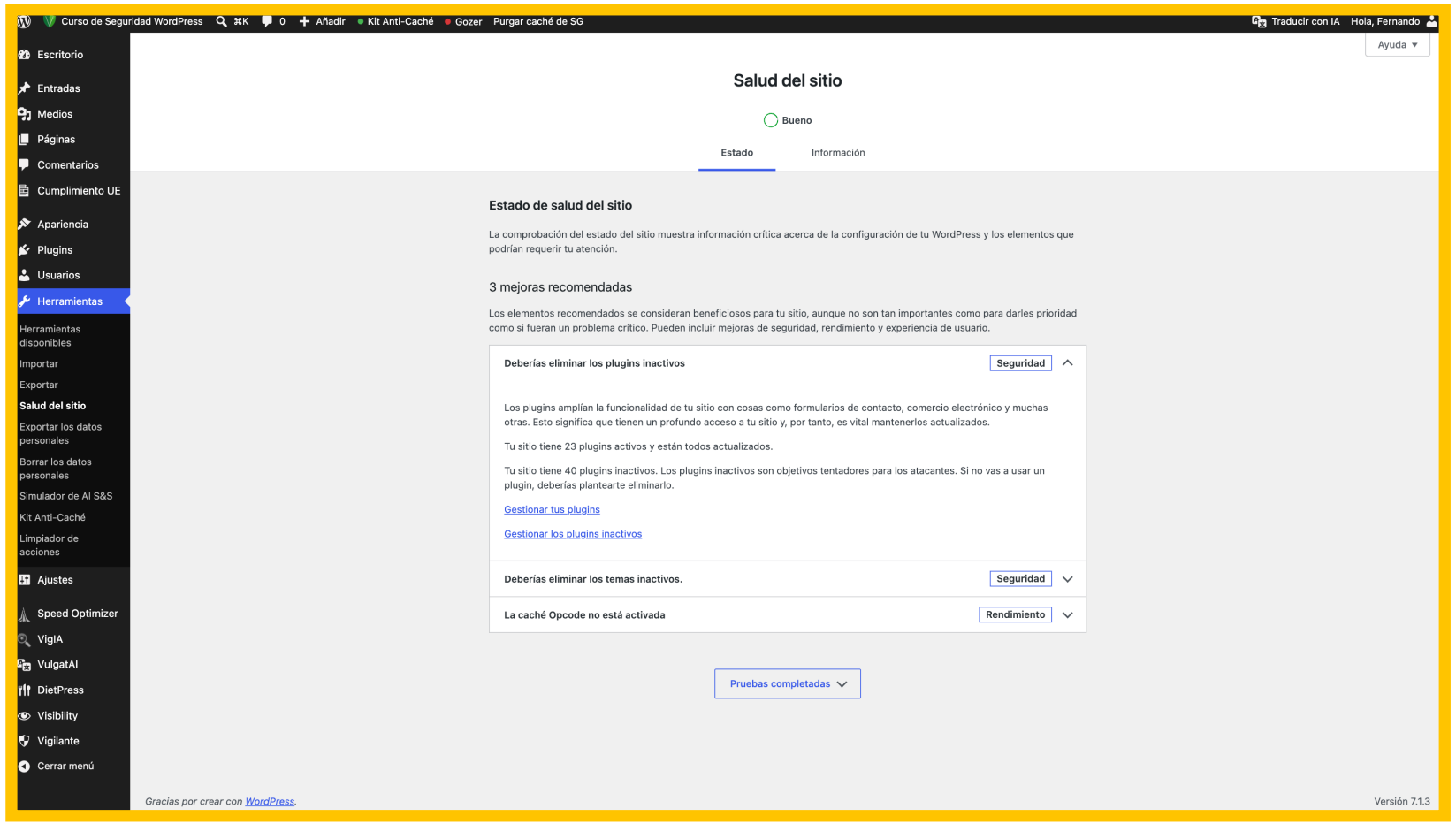
Cinco pantallas del escritorio que son seguridad

ACTO 1

1	**Salud del sitio**	Un auditor gratuito que casi nadie abre
2	[illegible]	[illegible]
3	[illegible]	[illegible]
4	[illegible]	[illegible]
5	[illegible]	[illegible]

Salud del sitio: el auditor que casi nadie abre

ACTO 1



Avisa de PHP sin soporte, plugins sin usar, depuración encendida o falta de HTTPS

Cada aviso explica cómo arreglarlo

Revisa configuración. No busca malware

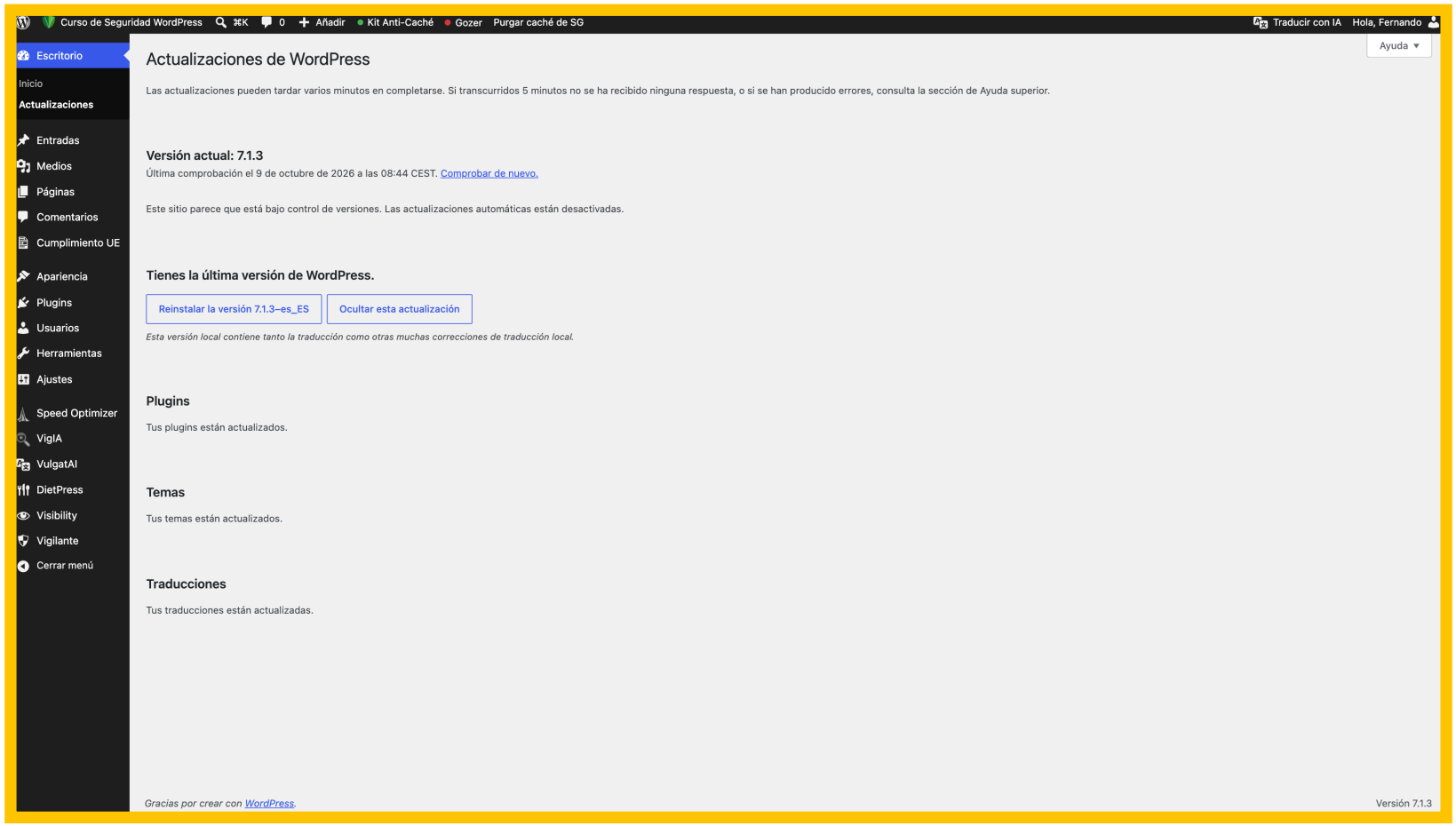
Cinco pantallas del escritorio que son seguridad

ACTO 1

1	**Salud del sitio**	Un auditor gratuito que casi nadie abre
2	**Actualizaciones**	El botón más eficaz de todo el escritorio
3	Ajustes generales	HTTPS, registro abierto y correo de administración
4	Tu perfil y usuarios	Sesiones, contraseñas de aplicación y roles
5	Comentarios	Pings, moderación y cierre de entradas antiguas

Actualizaciones: el botón más eficaz

ACTO 1



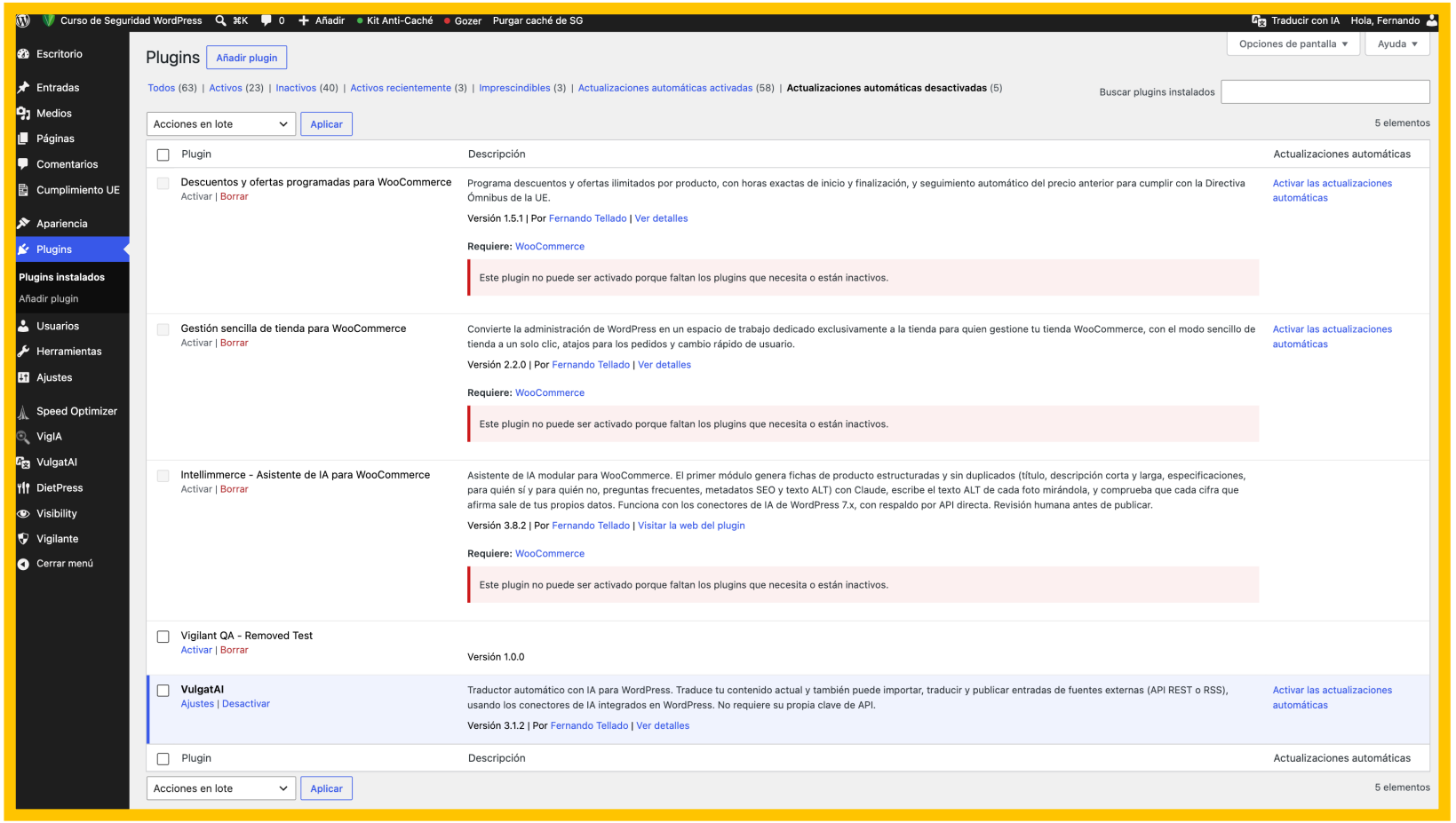
La mayoría de las intrusiones entran por algo sin actualizar

Reinstalar el núcleo: una copia limpia sin tocar tu contenido

Plugins y temas inactivos: bórralos

Actualizaciones automáticas, plugin a plugin

ACTO 1



Desde WordPress 5.5, en cada plugin y cada tema

Desde la 6.6, si una falla con error fatal, WordPress la revierte

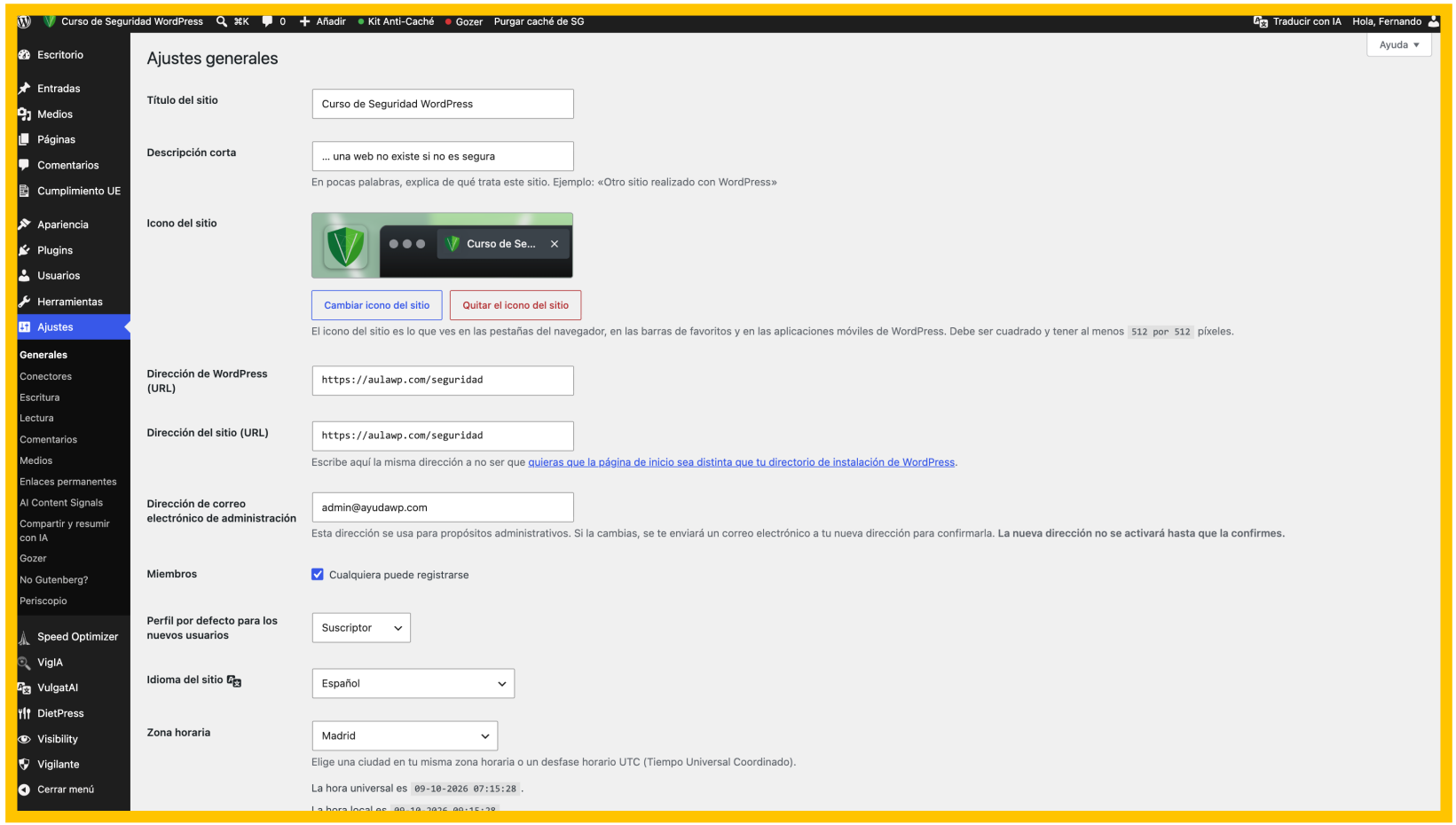
Cinco pantallas del escritorio que son seguridad

ACTO 1

1	**Salud del sitio**	Un auditor gratuito que casi nadie abre
2	**Actualizaciones**	El botón más eficaz de todo el escritorio
3	**Ajustes generales**	HTTPS, registro abierto y correo de administración
4	[illegible]	[illegible]
5	[illegible]	[illegible]

Ajustes generales: tres cosas

ACTO 1



Las dos direcciones, con https si tienes SSL activado

Registro abierto: mejor desactivado, sino perfil de suscriptor

Correo de admin: uno que leas (de verdad) a diario

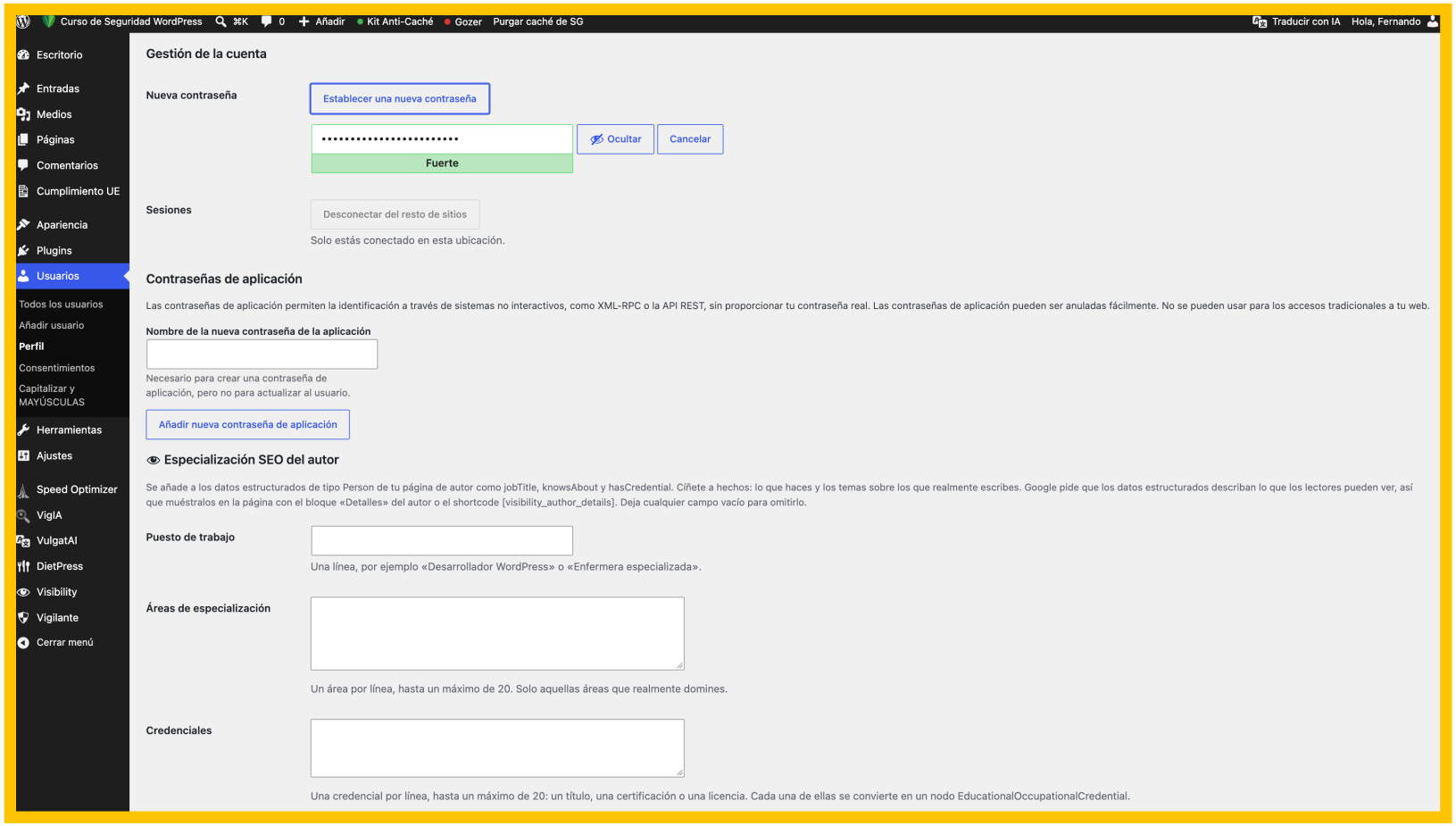
Cinco pantallas del escritorio que son seguridad

ACTO 1

1	**Salud del sitio**	Un auditor gratuito que casi nadie abre
2	**Actualizaciones**	El botón más eficaz de todo el escritorio
3	**Ajustes generales**	HTTPS, registro abierto y correo de administración
4	**Tu perfil y usuarios**	Sesiones, contraseñas de aplicación y perfiles
5	[illegible]	[illegible]

Tu perfil: sesiones y contraseñas de aplicación

ACTO 1



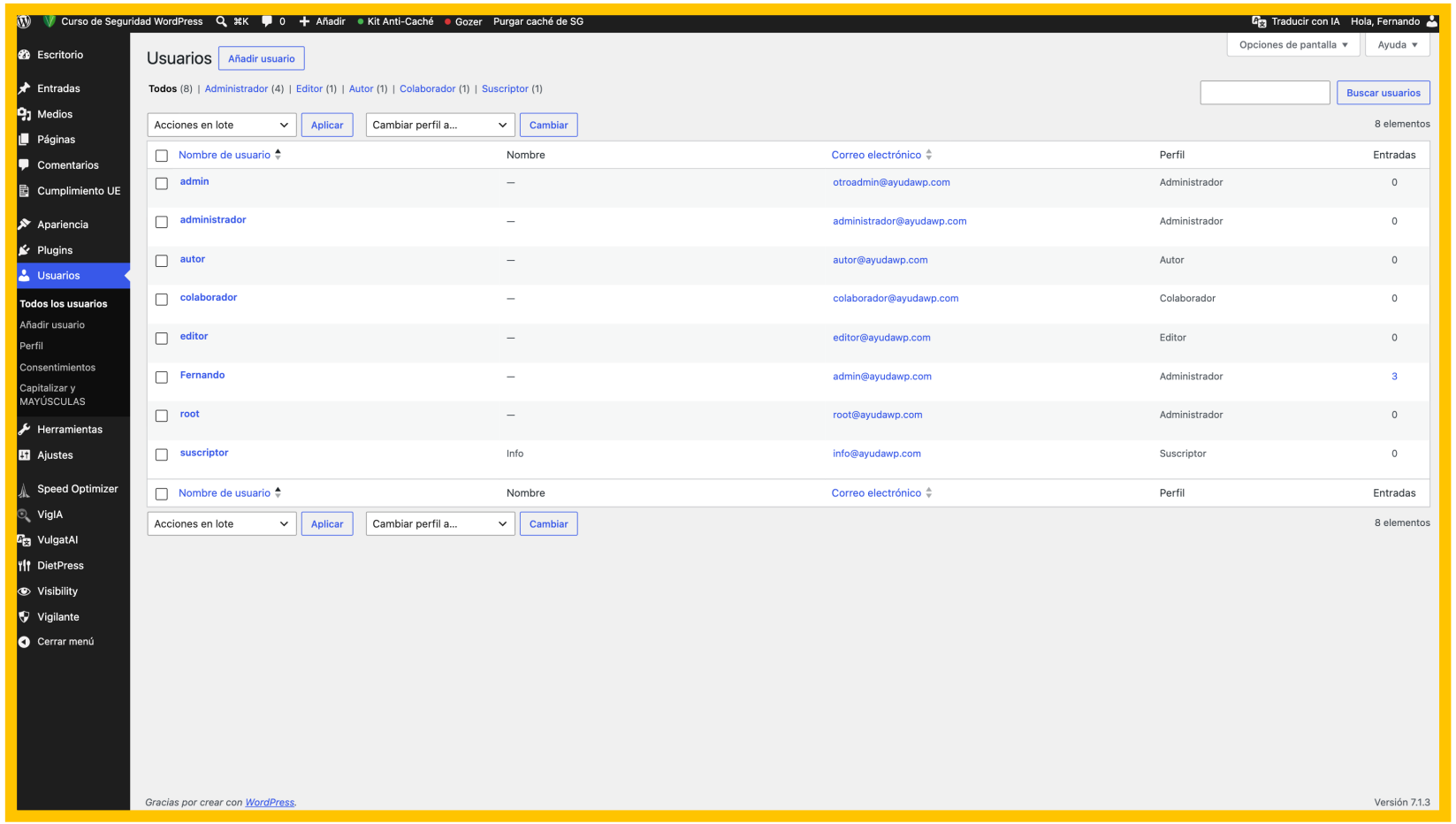
El nombre público no debe ser el de acceso

Cerrar sesión en todos los demás sitios

Contraseñas de aplicación: último uso e IP

¿Cuántos administradores hacen falta?

ACTO 1



Quien escribe es autor o editor

Menos administradores, menos daño si roban una cuenta

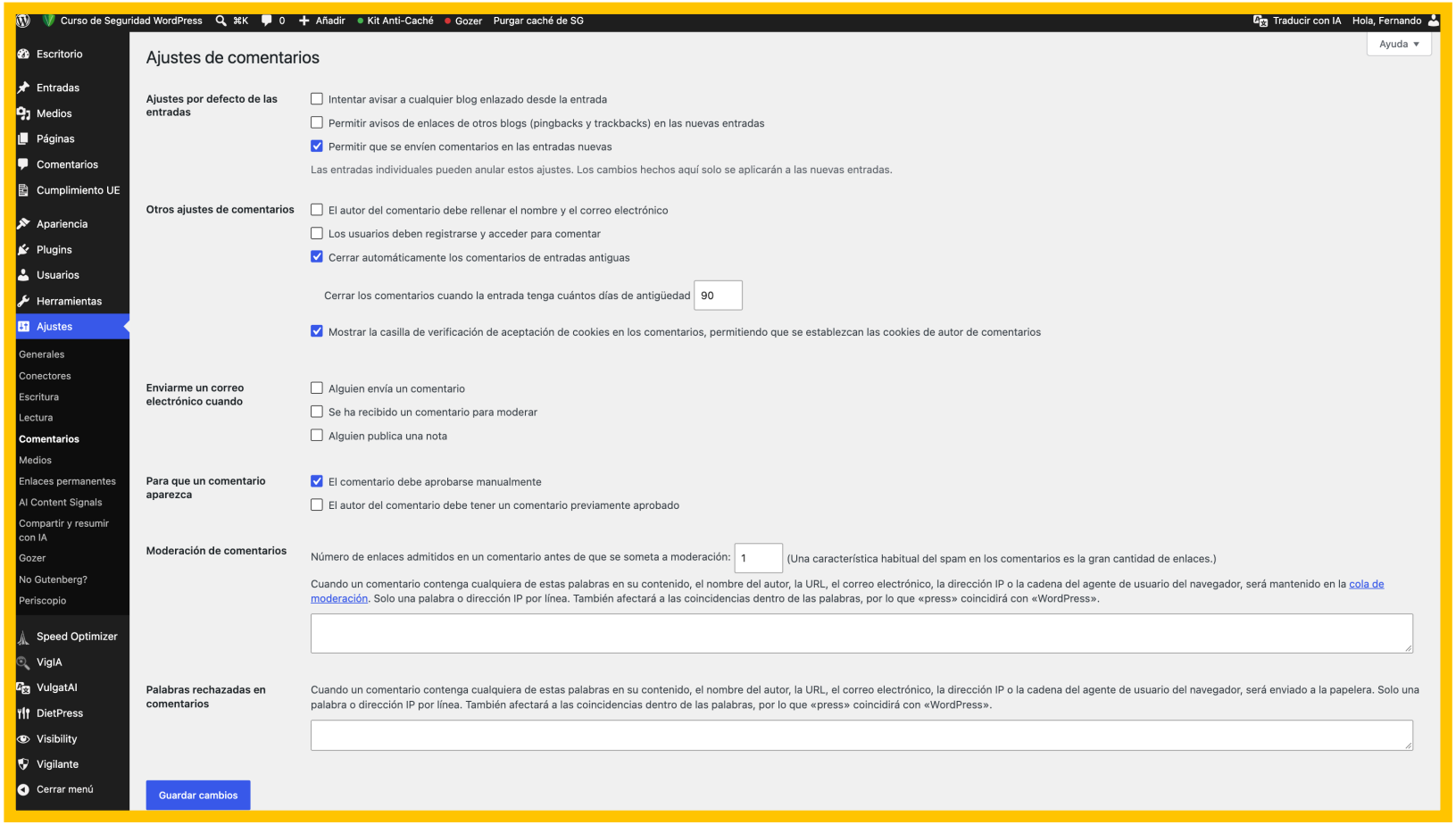
Cinco pantallas del escritorio que son seguridad

ACTO 1

1	**Salud del sitio**	Un auditor gratuito que casi nadie abre
2	**Actualizaciones**	El botón más eficaz de todo el escritorio
3	**Ajustes generales**	HTTPS, registro abierto y correo de administración
4	**Tu perfil y usuarios**	Sesiones, contraseñas de aplicación y perfiles
5	**Comentarios**	Pings, moderación y cierre de entradas antiguas

Comentarios: pingbacks y trackbacks fuera

ACTO 1



Primera línea contra los abusos de XML-RPC

Vaciar también los servicios de actualización

Cierra los pingbacks, no todo XML-RPC

Esas casillas solo afectan a las entradas nuevas

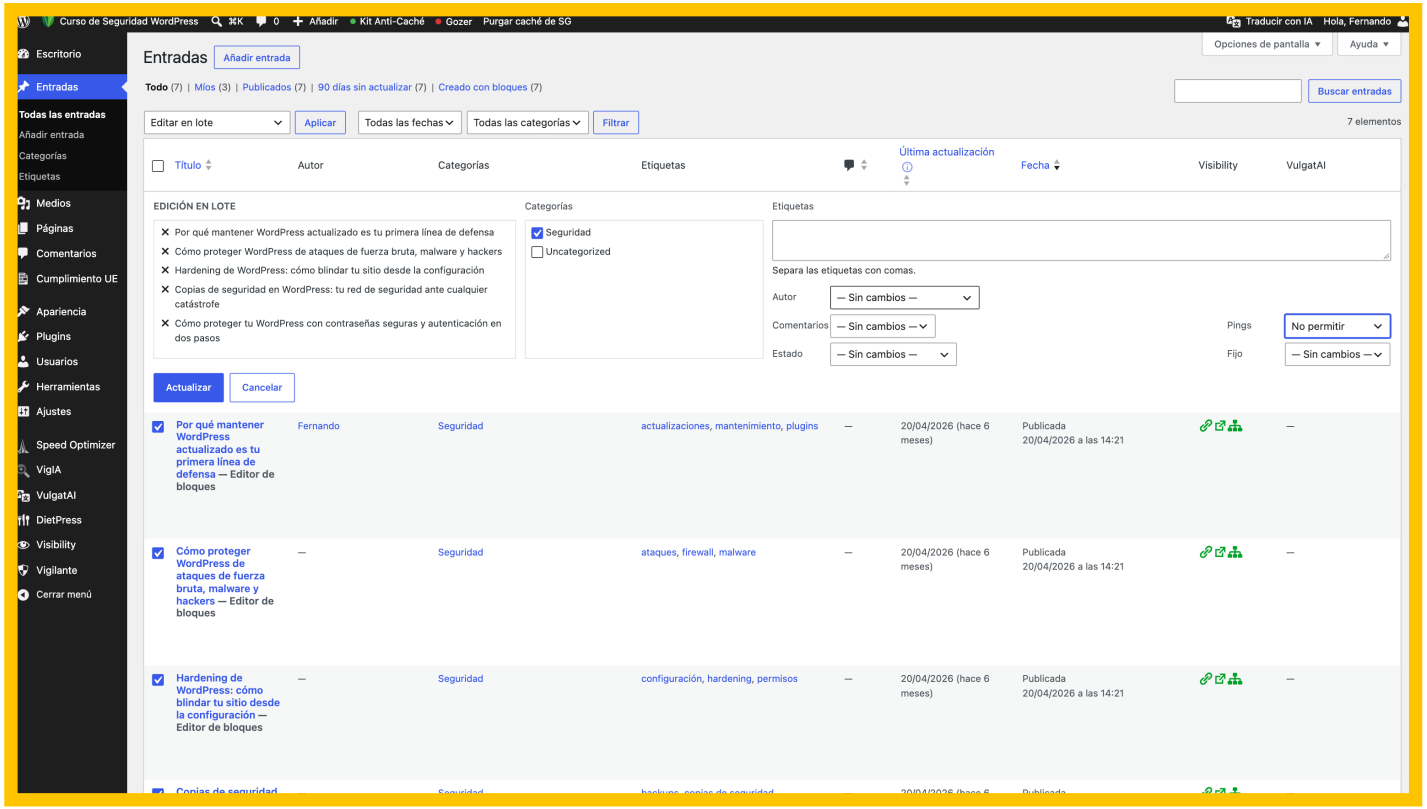
ACTO 1

Entradas nuevas

Aplican el ajuste y cierran los pings

Entradas ya publicadas

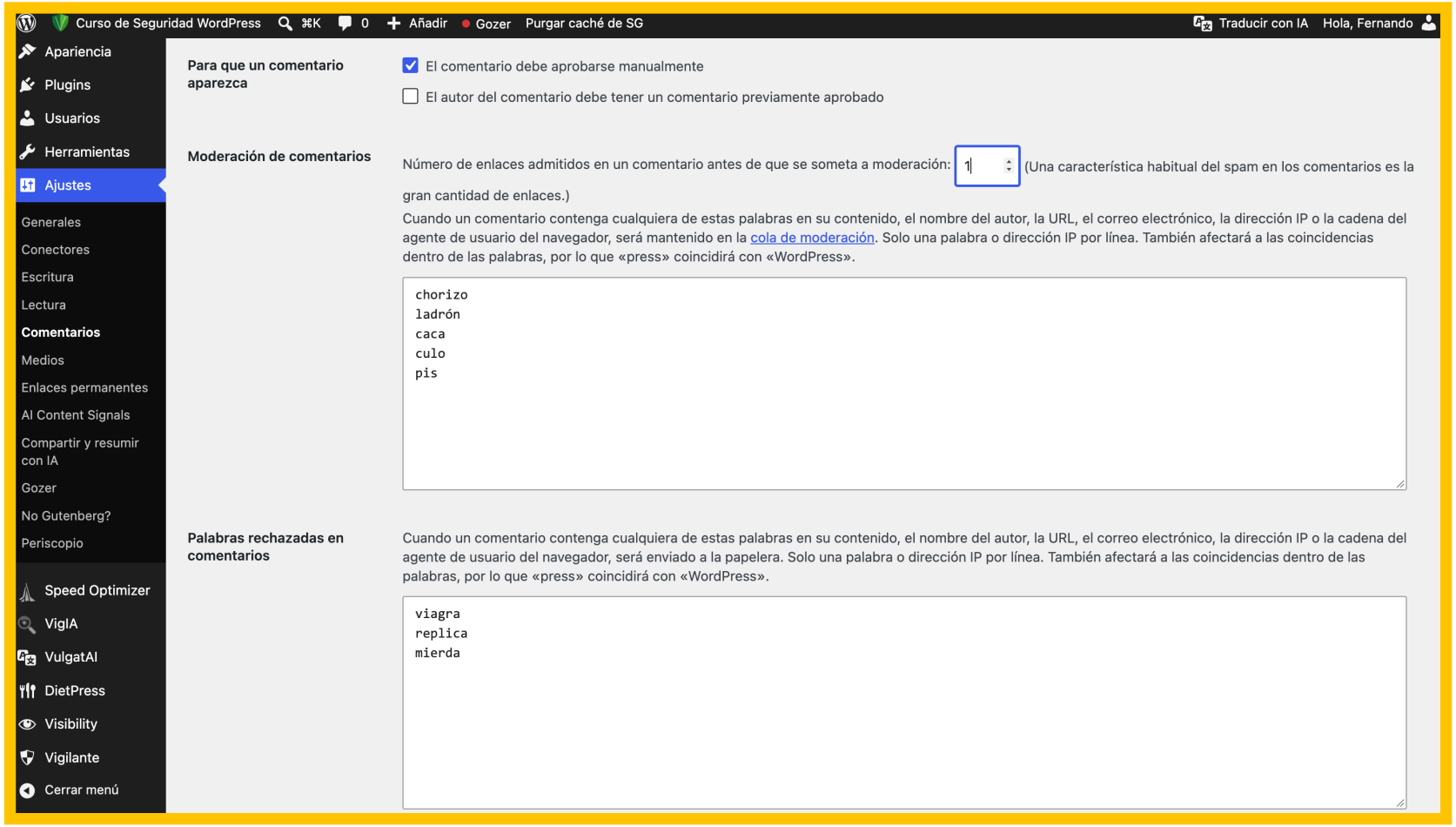
Conservan el ajuste de antes y siguen aceptando pingbacks



Edición en bloque: Seleccionar > Acciones > Editar > Pings: No permitir

Que todo comentario pase por moderación

ACTO 1



Aprobación manual, siempre activada

Cola para comentarios con dos o más enlaces

Cerrar comentarios en entradas antiguas

Palabras, dominios o IP a la papelera

ACTO 2

Lo que hace mal o le falta

Y cómo se arregla, de menos a más código

2

Qué falla y dónde se arregla

ACTO 2

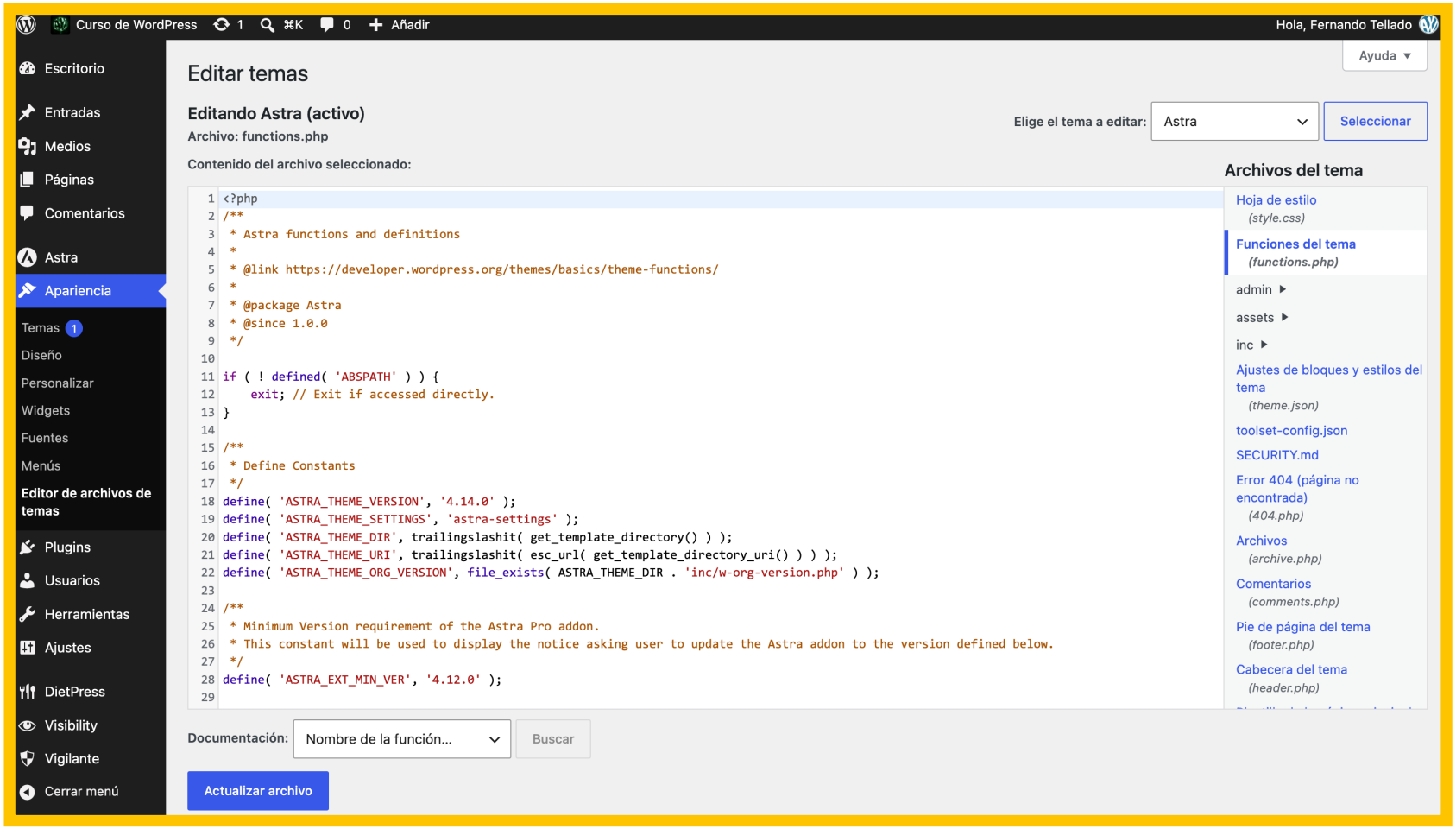
wp-config.php

- Editor de código dentro del escritorio
- Acceso y escritorio sin HTTPS forzado
- Depuración siempre activa
- HTML sin filtrar para administradores



Lo peor que trae WordPress: un editor de código

ACTO 2



Edita PHP desde el navegador, sin FTP

En manos de un administrador comprometido: código en tu servidor

Se quita con una línea

wp-config.php: el editor, fuera

ACTO 2

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

Sin editor de código en el escritorio. El primero que quitaría

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

Escritorio y acceso siempre por HTTPS

```
define( 'WP_DEBUG', false );
```

Nunca encendida en producción

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

Ni los administradores publican HTML sin filtrar

Contrapeso: quitar el editor no frena a un administrador comprometido, que aún puede instalar un plugin. Eso lo cierra DISALLOW_FILE_MODS, pero también bloquea las actualizaciones automáticas.

Después de un susto: claves y sales nuevas

ACTO 2

https://api.wordpress.org/secret-key/1.1/salt/

```
define('AUTH_KEY',         'K|n7a bGSd5;=y!AGl&hD$4yyNk{ Y(EENV3.+]{Sa*d1M#;RoRjQGGXmX2[:QSt');
define('SECURE_AUTH_KEY',  'SPN@#;}Po8bH h<k:;^jsd0~lU8F+?Apq5rqiaiJg:(fViuaI1uUatd%Von`!vJB');
define('LOGGED_IN_KEY',    'bj9[-13tQy}^%2x|x%)}cEf^S~)r3[85-y~!RT-4vS%9$.WySK2H+d,-d^G_|x*X');
define('NONCE_KEY',        '(|sN5WG+0?$dp Ah7U,_*6r=q@DDTXe?#z+HBBzJko;FP-H.9*P5[t1f+}djU9Fu');
define('AUTH_SALT',        '`kglM9b&&/QEl,#gMk-|#t/)&[YNpVX)7&vn(}Er`EKTx|k=yRNJ7P*P1nmkmiqA');
define('SECURE_AUTH_SALT', '1Tu%-4+w$)yna`[8-I</-Y#T}jsQO;[%?X%!R?vZYP}|(>O8fwsUA^|E6ie<uCSy');
define('LOGGED_IN_SALT',   'uStEqWJO6{pYv+ICq<xfNI-7^Scv{]:<p/Sh/m-xAPZVA/lT:|&3(!t9NYcl`Zv$');
define('NONCE_SALT',       'SIzD7001g`vkM?hBF`IM| uuQya^XrCpKi9bC(yMi|vy9$%~%s*|Ji&If@ERVn&S');
```

Ocho claves y salts nuevas

Cierra la sesión de todo el mundo, tú incluido

Qué falla y dónde se arregla

ACTO 2

wp-config.php

- Editor de código dentro del escritorio
- Acceso y escritorio sin HTTPS forzado
- Depuración encendida
- HTML sin filtrar para administradores

.htaccess

- PHP ejecutable en las subidas
- readme.html y license.txt
- Archivos .log, .sql y .bak
- XML-RPC abierto

.htaccess: PHP fuera de las subidas

ACTO 2

```
# wp-content/uploads/.htaccess
<FilesMatch "\.(php[0-9]*|phtml|phar)$">
    Require all denied
</FilesMatch>
```

Un .php subido no se ejecuta (también .php5, .phtml y .phar)

La entrada más típica: un archivo disfrazado de imagen

.htaccess: la raíz

ACTO 2

```
# .htaccess de la raíz
Options -Indexes
<FilesMatch "^(readme\.html|license\.txt|wp-config-sample\.php|wp-config\.php)$">
    Require all denied
</FilesMatch>
<FilesMatch "\.(log|sql|bak)$">
    Require all denied
</FilesMatch>
# Solo si no usas la app móvil ni Jetpack:
<Files xmlrpc.php>
    Require all denied
</Files>
```

Sin listado de carpetas, sin readme ni license, sin .log, .sql ni .bak

xmlrpc.php cortado en el servidor, si no usas Jetpack ni la app móvil

Qué falla y dónde se arregla

ACTO 2

wp-config.php

- Editor de código dentro del escritorio
- Acceso y escritorio sin HTTPS forzado
- Depuración encendida
- HTML sin filtrar para administradores

.htaccess

- PHP ejecutable en las subidas
- readme.html y license.txt
- Archivos .log, .sql y .bak
- XML-RPC abierto

Un archivo PHP

- Nombres de usuario visibles
- Errores que delatan al usuario
- Sesiones de 2 y 14 días
- Sin cabeceras de seguridad

Un único archivo en mu-plugins

ACTO 2

`ayudawp-hardening.php`

Acceso

- Límite de intentos por IP
- Mismo error exista o no el usuario
- Sesiones más cortas
- XML-RPC y pings cerrados

Usuarios

- ?author= y API REST cerrados
- Mapa del sitio sin usuarios
- Nombres reservados
- Aviso si aparece un administrador

Cabeceras

- Cinco cabeceras en una función
- Antes y después en securityheaders.com

Vigilar y limpiar

- Escaneo diario de PHP en las subidas
- Fuera la versión del código

Acceso: límite de intentos

ACTO 2

```php
add_action( 'wp_login_failed', 'ayudawp_track_failed_login', 10, 2 );
add_filter( 'authenticate', 'ayudawp_block_locked_ip', 99, 3 );

function ayudawp_block_locked_ip( $user, $username, $password ) {
    // $data = fallos de esta IP, guardados en un transitorio
    if ( $data['count'] >= 5 && $data['until'] > time() ) {
        return new WP_Error( 'ayudawp_locked',
            'Demasiados intentos fallidos. Vuelve a probar en unos minutos.' );
    }
    return $user;
}
```

Bloquea aunque la contraseña sea la correcta

Prioridad 99, no 1: si no, la contraseña correcta lo salta

Detrás de un proxy, el servidor debe dar la IP real

Acceso: el mismo error y sesiones más cortas

ACTO 2

```php
// El mismo error exista o no el usuario
add_filter( 'authenticate', function ( $user ) {
    if ( is_wp_error( $user ) && /* usuario, correo o contraseña incorrectos */ ) {
        return new WP_Error( 'authentication_failed',
            'Usuario, correo o contraseña incorrectos.' );
    }
    return $user;
}, 100 );

// Sesiones: 12 horas, o 3 días con «Recuérdame» (WordPress: 2 y 14 días)
add_filter( 'auth_cookie_expiration', function ( $seconds, $user_id, $remember ) {
    return $remember ? 3 * DAY_IN_SECONDS : 12 * HOUR_IN_SECONDS;
}, 10, 3 );
```

No delata si el usuario existe

Un portátil perdido ya no sirve dos semanas

La recuperación de contraseña del núcleo sí lo delata

Acceso: XML-RPC, pings y contraseñas de aplicación

ACTO 2

```php
// XML-RPC cerrado: sin acceso con usuario y sin ningún método
add_filter( 'xmlrpc_enabled', '__return_false' );
add_filter( 'xmlrpc_methods', '__return_empty_array' );

// O abierto para Jetpack o la app móvil, pero sin pingbacks
add_filter( 'xmlrpc_methods', function ( $methods ) {
    unset( $methods['pingback.ping'], $methods['pingback.extensions.getPingbacks'] );
    return $methods;
} );

// Pings cerrados en todas las entradas, viejas y nuevas
add_filter( 'pings_open', '__return_false', 20 );

// Sin contraseñas de aplicación si no usas integraciones externas
add_filter( 'wp_is_application_passwords_available', '__return_false' );
```

xmlrpc_enabled solo corta lo que pide login: por eso se vacían también los métodos

Pings cerrados en todas las entradas, viejas y nuevas

Usuarios: ?author= y API REST

ACTO 2

```php
add_action( 'template_redirect', 'ayudawp_block_author_scan', 1 );

function ayudawp_block_author_scan() {
    if ( isset( $_GET['author'] ) && is_numeric( $_GET['author'] ) ) {
        wp_safe_redirect( home_url( '/' ), 301 );
        exit;
    }
}

add_filter( 'rest_endpoints', function ( $endpoints ) {
    if ( ! is_user_logged_in() ) {
        unset( $endpoints['/wp/v2/users'] );  // y la ruta de un solo usuario
    }
    return $endpoints;
} );
```

?author=1 manda a la portada

Prioridad 1: antes de la redirección de WordPress

Si una app lee usuarios sin sesión, la rompe

Usuarios: mapa del sitio, nombres y aviso

ACTO 2

```php
// Fuera los usuarios del mapa del sitio
add_filter( 'wp_sitemaps_add_provider', function ( $provider, $name ) {
    return ( 'users' === $name ) ? false : $provider;
}, 10, 2 );

// Nombres reservados: admin, root, test... (solo los que nadie usa ya)
add_filter( 'illegal_user_logins', 'ayudawp_reserved_usernames' );

// Un correo cuando alguien recibe el rol de administrador
add_action( 'add_user_role', 'ayudawp_alert_on_admin_promotion', 10, 2 );
```

El mapa del sitio ya no lista usuarios

Nombres reservados, pero no los que ya existen

Un correo el día que alguien recibe el rol de administrador

Cabeceras de seguridad

ACTO 2

```
add_action( 'send_headers', 'ayudawp_security_headers' );

function ayudawp_security_headers() {
    header( 'X-Content-Type-Options: nosniff' );
    header( 'X-Frame-Options: SAMEORIGIN' );
    header( 'Referrer-Policy: strict-origin-when-cross-origin' );
    header( 'Permissions-Policy: camera=(), microphone=(), geolocation=()' );
    if ( is_ssl() ) { header( 'Strict-Transport-Security: max-age=31536000' ); }
}
```

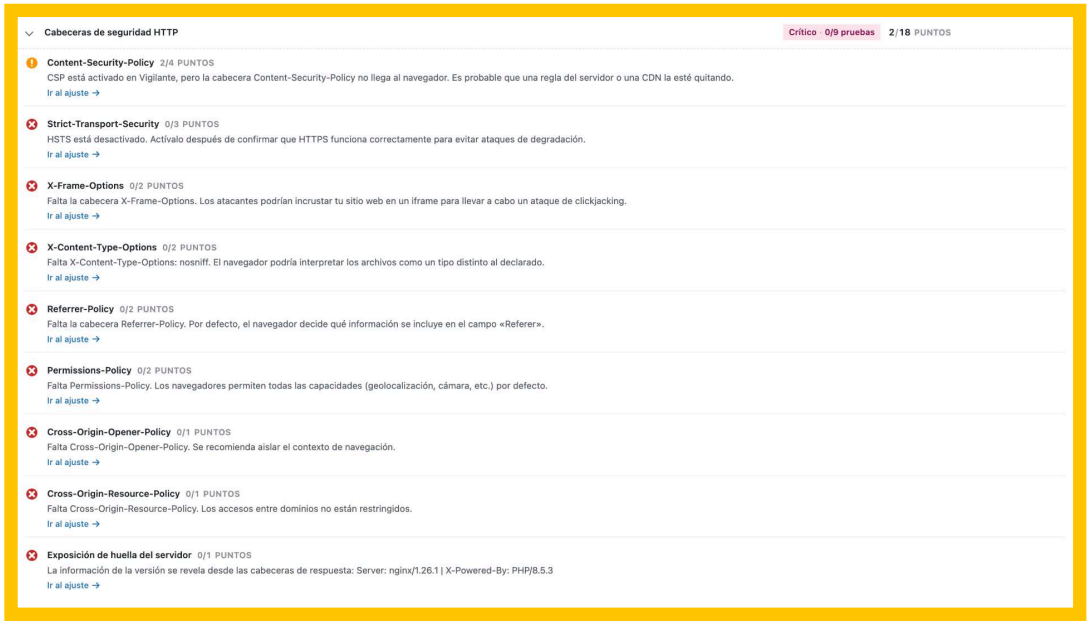
Cinco cabeceras en una función

HSTS: el navegador se acuerda un año

Content Security Policy se queda fuera

Cabeceras: antes y después

ACTO 2





Antes

Después

Sin tocar nada más, solo con cinco líneas en un archivo

Vigilar y limpiar

ACTO 2

```php
// Cada día: archivos PHP dentro de las subidas (no debería haber ninguno)
wp_schedule_event( time() + HOUR_IN_SECONDS, 'daily', 'ayudawp_daily_scan' );
// ... recorre la carpeta de subidas, junta los *.php y manda la lista por correo

// Limpieza: sin la versión de WordPress en el código de la página
remove_action( 'wp_head', 'wp_generator' );
remove_action( 'wp_head', 'rsd_link' );
add_filter( 'the_generator', '__return_empty_string' );
// ?ver= fuera, solo en los archivos del núcleo
add_filter( 'style_loader_src', 'ayudawp_remove_version_query', 9999 );
add_filter( 'script_loader_src', 'ayudawp_remove_version_query', 9999 );
```

Un correo si aparece un .php en las subidas

Limpieza: capa extra, no un escudo

Qué falla y dónde se arregla

ACTO 2

wp-config.php

- Editor de código dentro del escritorio
- Acceso y escritorio sin HTTPS forzado
- Depuración encendida
- HTML sin filtrar para administradores

.htaccess

- PHP ejecutable en las subidas
- readme.html y license.txt
- Archivos .log, .sql y .bak
- XML-RPC abierto

Un archivo PHP

- Nombres de usuario visibles
- Errores que delatan al usuario
- Sesiones de 2 y 14 días
- Sin cabeceras de seguridad

Vigilante

- Límite de intentos de acceso
- 2FA
- Cortafuegos
- Vigilancia de archivos
- Auditoría y avisos

Lo que no se arregla con cuatro funciones

ACTO 2



Autorización 2FA completa

Email, códigos TOTP, lectura de QR y dispositivos de confianza



Una URL de acceso propia

Con reglas de rewrite y excepciones personalizadas



Un cortafuegos con reglas

Los patrones caseros dan falsos positivos y no se actualizan solos

Para esto entra Vigilante

ACTO 3

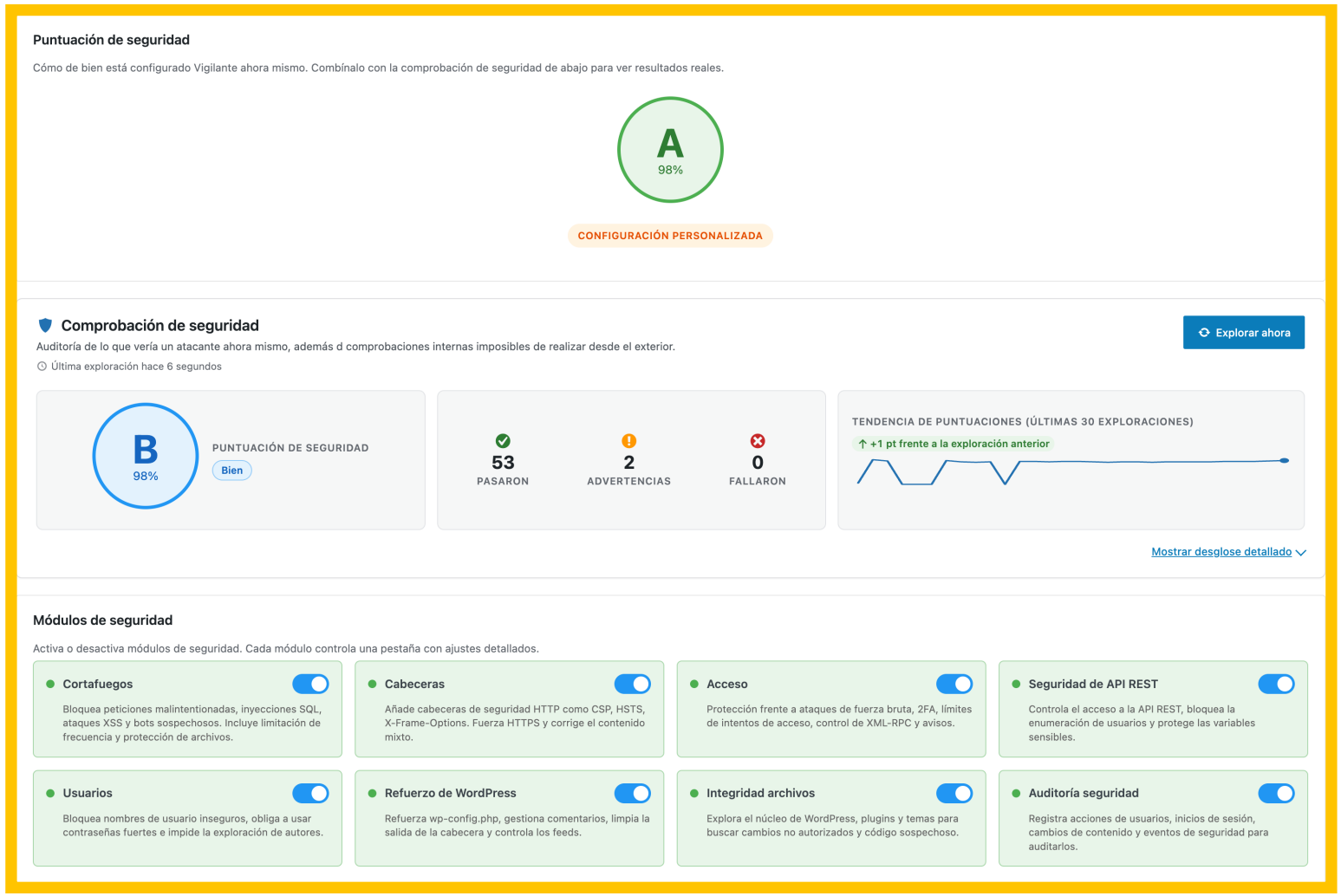
Vigilante, para comprobarlo todo

Gratuito y sin versión de pago

3

Lo de hoy, con clics

ACTO 3



Gratuito, sin versión de pago

Dos preajustes: Estándar y Máxima seguridad

Descarga antes una copia de wp-config.php y .htaccess

La Comprobación de seguridad

ACTO 3

50+
comprobaciones

6
categorías

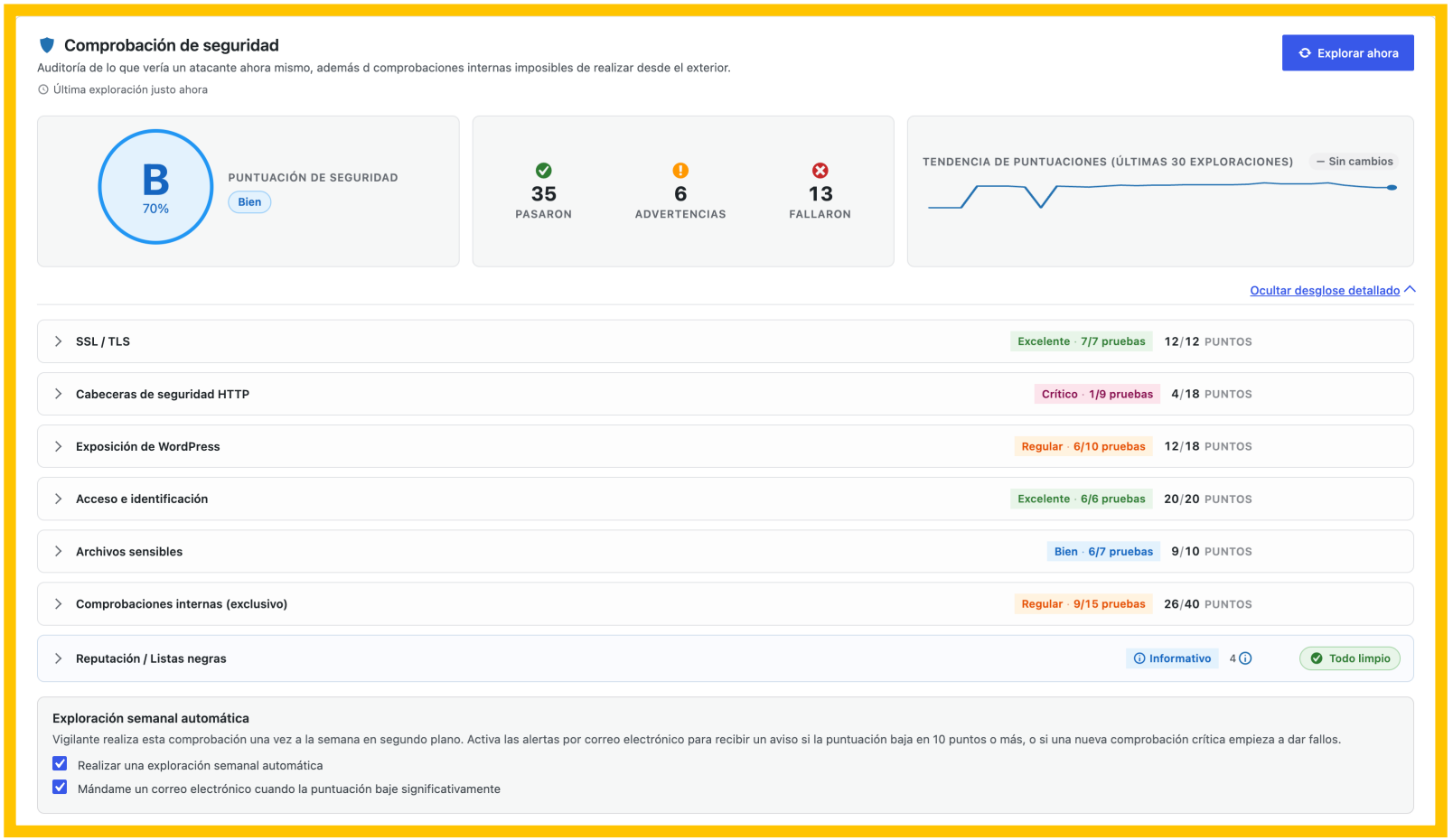
0-100
nota, de la A a la E

- SSL/TLS
- Cabeceras HTTP
- Exposición de WordPress
- Acceso e identificación
- Archivos sensibles
- Comprobaciones internas

Corre en tu servidor, sin cuentas ni claves de ningún servicio

La nota, a la vista

ACTO 3



Nota de 0 a 100 y calificación de A a E

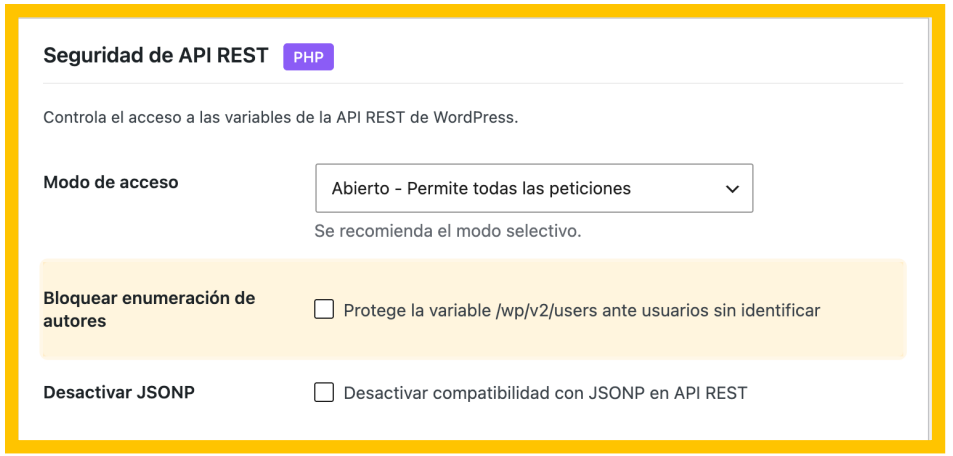
Verde: lo que ve en el sitio en vivo

Rojo: lo que falta, o lo que el plugin no puede ver

Del fallo a la casilla, en un clic

ACTO 3





El fallo

Cada fallo lleva directo a la casilla que lo arregla

La casilla

Donde el código no alcanza

ACTO 3



Identificación en dos pasos

Aplicación o correo, con códigos de recuperación



URL de acceso propia

Oculta wp-login.php a los bots



Cortafuegos y modo Bajo ataque

Reglas, listas de IP y emergencia que se apaga a las 4 horas



Vigilancia de archivos

Núcleo, plugins, temas y subidas, con aviso por correo



Auditoría con alertas

Quién hizo qué, y avisos cuando algo grave pasa



Dos preajustes

Estándar y Máxima seguridad, a un clic

Nada de esto cuesta ni un euro

¡De nada!



Ajustes del escritorio, wp-config.php, .htaccess y un archivo PHP. Y Vigilante para comprobarlo todo.

Seguridad en WordPress con presupuesto cero



Meetup WordPress Coruña

Fernando Tellado · AyudaWP.com · @fernandot

github.com/fernandotellado/meetup-coruna-2026