

# 1º Versión del Core.

El primer punto es revisar en qué versión se encuentra nuestro Wordpress, mantener actualizado el core de WordPress es una medida esencial de seguridad y estabilidad. Cada versión nueva corrige vulnerabilidades conocidas que, de no solucionarse, pueden ser explotadas por atacantes. Además, estas actualizaciones incluyen optimizaciones de rendimiento y compatibilidad con nuevos estándares de PHP, MySQL y navegadores, lo que reduce errores y riesgos de incompatibilidad con plugins o temas.

También aseguran que el sitio cumpla con prácticas seguras de codificación promovidas por la comunidad de desarrollo. En un protocolo de seguridad, la revisión y actualización periódica del core debe ser prioritaria para garantizar la integridad de la plataforma.

La periodicidad recomendada para actualizar el core de WordPress depende del tipo de actualización. Las actualizaciones críticas de seguridad deben aplicarse de forma inmediata (idealmente en menos de 24 horas); las versiones mayores pueden instalarse tras realizar pruebas en un entorno de staging\* y esperar algunas horas o días para evitar conflictos con plugins o temas.

Como buena práctica, debe revisarse la disponibilidad de nuevas versiones al menos una vez por semana y programar la actualización manual tan pronto se publique una versión estable.

\**Staging:* Un entorno de staging en WordPress es una copia exacta del sitio web principal que funciona como un espacio seguro y privado de pruebas. Permite experimentar, actualizar o modificar configuraciones, plugins y temas sin afectar la web en producción ni a sus usuarios.

## Acciones

Desde el botón Inicio> Actualizaciones podemos ver la versión del core de nuestro sitio Wordpress, en nuestro caso está todo correcto en la última versión:

**Versión actual: 6.8.2**

Última comprobación el 24 de septiembre de 2025 a las 08:32 GMT+0000. [Comprobar ahora](#)

Este sitio se mantiene actualizado automáticamente con cada nueva versión de WordPress. Puedes [cambiar a actualizaciones automáticas solo para versiones de mantenimiento](#).

**Tienes la última versión de WordPress.**

[Reinstalar la versión 6.8.2-es\\_ES](#)   [Ocultar esta actualización](#)

Esta versión local contiene tanto la traducción como otras muchas correcciones de traducción

## 2. Actualización de Temas

Actualizar todos los temas instalados en WordPress, incluidos los que no están activos, es una medida clave para la seguridad del sitio. Las versiones desactualizadas pueden contener vulnerabilidades que los atacantes explotan para obtener acceso no autorizado o instalar malware, aunque el tema no esté activo en producción. Además, los temas sin actualizar pueden provocar incompatibilidades con nuevas versiones de WordPress, causando errores o caídas del sitio.

Las actualizaciones también incluyen parches de funcionalidad y mejoras de rendimiento que mantienen el sitio eficiente y ágil. No actualizar incrementa el riesgo de pérdida de datos, suplantación de identidad y bloqueos del sitio por ataques automatizados.

Por razones de higiene digital y para reducir la superficie de ataque, se recomienda también eliminar aquellos temas que no sean necesarios. Antes de actualizar, es recomendable realizar una copia de seguridad completa y verificar el resultado en un entorno de staging, si es posible. Mantener todos los temas al día garantiza la integridad, estabilidad, compatibilidad y máxima protección frente a amenazas externas.

### Acciones

Aquí nos encontramos con 3 temas de los cuales se está usando solo 1. Por lo cual clicamos en los temas inactivos, más detalles, y borramos. De esta forma reducimos la posible superficie de ataque.

The screenshot shows the WordPress Themes dashboard. At the top, there are buttons for 'Temas' (3), 'Añadir tema', and a search bar 'Buscar temas instalados'. Below the search bar, there's a button 'Actualizar ahora' (Available update). The dashboard lists three themes:

- GeneratePress**: Status: **Activo**. Description: 'Welcome to GeneratePress'. It shows a preview of a modern website design with a blue header and footer. Below the preview are sections for 'Who We Are', 'What We Do', and 'How We Do It'. A note at the bottom says 'Aktivo: GeneratePress'.
- Twenty Twenty-Five**: Status: **Inactivo**. Description: 'Nueva versión disponible. [Actualizar ahora](#)'. It shows a preview of a website with a red background and two birds on a branch. Below the preview is a note: 'Twenty Twenty-Five is a clean and modern theme designed for personal blogs and portfolios. It features a minimalist design with a focus on readability and a clean layout. The theme includes a variety of page templates and a responsive design that looks great on all devices.'
- Twenty Twenty-Four**: Status: **Inactivo**. Description: 'A commitment to innovation and sustainability'. It shows a preview of a website with a blue background and a large image of a building with a unique curved roof. Below the preview is a note: 'Twenty Twenty-Four is a pioneering theme that seamlessly merges creativity and functionality. It's built with performance in mind, featuring a fast-loading, SEO-friendly design that's perfect for modern websites.'

## NOTA

En Ajustes>Medios se debe poner a 0 los valores para evitar generar más imágenes de la cuenta y esto ralentice por problemas de espacio.

### 3. Actualización de plugins en WordPress

Actualizar los plugins en WordPress es una práctica técnica fundamental para garantizar la seguridad, estabilidad y rendimiento del sitio. Los plugins desactualizados pueden contener vulnerabilidades explotables que permiten a hackers obtener acceso no autorizado o injectar código malicioso. Además, las actualizaciones corigen errores y mejoran la compatibilidad con el core de WordPress y otros plugins, previniendo conflictos que podrían causar fallos o caídas del sitio. Los plugins abandonados **que no reciben mantenimiento ni actualizaciones representan un riesgo crítico**, pues sus vulnerabilidades no se parchean.

Para evaluar la seguridad de los plugins, es recomendable auditar regularmente la lista instalada, eliminar los que estén desactualizados o abandonados, y sustituirlos por alternativas mantenidas activamente. Se deben usar herramientas especializadas para detectar vulnerabilidades y probar la compatibilidad entre plugins antes de aplicar actualizaciones en producción, idealmente mediante un entorno de staging.

#### → Identificación de plugins con mayor riesgo de vulnerabilidad en WordPress

Los plugins representan uno de los principales vectores de ataque en WordPress debido a su complejidad y diversidad. Para identificar plugins de alto riesgo se aconseja:

- Mantener los *plugins* siempre *actualizados*; las versiones desactualizadas son las más vulnerables y comunes en ataques.
- Detectar *plugins abandonados*, es decir, sin soporte ni actualizaciones recientes, ya que sus vulnerabilidades permanecen sin parchear.
- Utilizar *herramientas especializadas* de escaneo de seguridad, como WPScan, Wordfence, Sucuri o WPNeurona, que analizan versiones instaladas y reportan vulnerabilidades conocidas, además de detectar malware o actividad sospechosa.

- Revisar *bases de datos públicas* de vulnerabilidades como WPScan Vulnerability Database o CVE (Common Vulnerabilities and Exposures) para conocer problemas reportados en plugins específicos.
- Monitorear el estado de seguridad del sitio mediante *plugins de salud y seguridad* que informan si hay posibles brechas en plugins activos.
- Realizar *auditorías regulares* y actualizar o desactivar plugins vulnerables o innecesarios.

## → Qué herramientas recomendadas puedo usar para analizar la compatibilidad de plugins

Para analizar la compatibilidad de plugins en WordPress, se recomiendan herramientas específicas que ayudan a detectar posibles conflictos y problemas antes de aplicar actualizaciones en producción. Algunas de las herramientas más destacadas son:

- [PHP Compatibility Checker](#): Escanea plugins y temas para verificar su compatibilidad con diferentes versiones de PHP. Proporciona informes detallados de errores y advertencias que pueden impedir su correcto funcionamiento en versiones específicas de PHP.
- [Better Plugin Compatibility Control](#): Presenta visualmente la compatibilidad de cada plugin instalado con la versión actual de WordPress y PHP, útil para administradores no técnicos por su facilidad de uso.
- [Plugin Compatibility Checker](#): Herramienta más avanzada que realiza análisis exhaustivos en tiempo real para sitios complejos, mostrando resultados detallados dentro del panel de administración.
- [Herramientas de prueba locales como DevKinsta](#): Permiten crear entornos locales para realizar pruebas con distintas combinaciones de plugins, temas y versiones de PHP sin afectar el sitio en producción.

Adicionalmente, existen plugins y herramientas que identifican conflictos entre plugins mediante análisis de código, sugiriendo soluciones para mitigar incompatibilidades.

Si se desea, se puede guiar en la instalación y uso de alguna de estas herramientas para analizar la instalación específica y detectar riesgos o incompatibilidades.

Según el listado de plugins que tiene el wordpress, no he encontrado incompatibilidades críticas documentadas entre ellos. La mayoría son ampliamente utilizados, bien mantenidos y reconocidos como seguros siempre que estén actualizados. Sin embargo, hay algunas consideraciones de seguridad y recomendaciones:

- Los plugins de seguridad como **Wordfence Security** y **WPS Hide Login** pueden entrar en conflicto si ambos modifican aspectos del login/acceso, aunque no es común; siempre hay que verificar tras las actualizaciones de estos.
- **GP Premium** o **GenerateBlocks** pueden tener incompatibilidad con otros constructores visuales, pero en este caso no hay otros constructores activos reportados.
- **H5P**, **Genially Embed** y **PDF Poster** agregan funcionalidades externas; verifican actualizaciones constantes para evitar vulnerabilidades en la manipulación de contenido embebido.
- **IONOS Performance** y **Under Construction** raramente causan problemas, pero es recomendable actualizar y consultar documentación si aparecen bloqueos inesperados.
- **Spectra**, **GenerateBlocks**, **GP Premium** y **Bloque de carrusel de diapositivas** son plugins de bloques y generalmente funcionan bien juntos, siempre y cuando no intentes modificar el mismo elemento de la página al mismo tiempo.

Respecto a peligrosidad:

- Los plugins de respaldo (UpdraftPlus) y seguridad (Wordfence Security, WPS Hide Login) son críticos y deben mantenerse siempre en su última versión para evitar brechas.
- Plugins que permiten subir o embeber contenido (H5P, PDF Poster, Genially Embed) deben usarse con precaución y restringir los permisos para evitar cargas o ejecuciones inseguras.
- Under Construction no representa riesgo, pero nunca debe quedar activado indefinidamente ya que bloquea el acceso público al sitio.

## Acciones

En este apartado tomaría una decisión sobre qué plugins son necesarios y cuáles no para poder eliminar los que no sirvan así como plugins que están desactivados.

## Plugins y su función

Plugin	Función principal	¿Se puede eliminar?

Advanced Google reCAPTCHA	Protege formularios contra bots y spam usando el sistema de captcha de Google.	No, mantener para evitar registros falsos.
Akismet Anti-spam: Spam Protection	Filtrado automático de comentarios spam en entradas y formularios.	No, salvo que uses otro anti-spam.
Bloque de carrusel de diapositivas	Añade carruseles/galerías de imágenes como bloques en el editor.	Eliminar si no necesitas sliders.
GenerateBlocks	Constructor de bloques visuales, permite maquetar páginas con bloques editables avanzados.	Prescindible si usas otro visual builder.
<b>Genially Embed</b>	<b>Permite insertar creaciones interactivas de Genially fácilmente en tus páginas.</b>	<b>Eliminar si no incrustas contenidos Genially.</b>
GP Premium	Extiende el tema GeneratePress con más opciones de diseño y funcionalidades premium.	Mantener si tu tema es GeneratePress.
H5P	Permite crear, insertar y gestionar contenidos interactivos como quizzes, vídeos, etc.	Eliminar si no usas este tipo de contenidos.

IONOS Performance	Optimiza velocidad/rendimiento (generalmente para sitios en hosting IONOS).	Eliminar si no usas hosting IONOS o tienes otro optimizador.
PDF Poster	Insertar y visualizar archivos PDF directamente en las páginas del sitio.	Eliminar si nunca embebes PDFs.
Spectra	Otro plugin de bloques visuales (constructor/editor visual).	Prescindible si usas GenerateBlocks o viceversa.
Under Construction	Permite mostrar una página “En construcción” a los visitantes, útil en mantenimientos.	Eliminar si tu web está ya publicada.
UpdraftPlus - Backup/Restore	Creación y restauración fácil de copias de seguridad automáticas.	Mantener siempre para seguridad.
Wordfence Security	Firewall y antivirus; protege contra malware, ataques, fuerza bruta y además incluye 2FA.	Mantener siempre para máxima seguridad.
WPS Hide Login	Permite cambiar la URL de acceso al panel para evitar ataques automatizados contra	Mantener si deseas protección extra en login.

<input type="checkbox"/> <b>GP Premium</b>	Toda la co
<a href="#">Desactivar</a>   <a href="#">Configurar</a>	Versión 2
<div style="background-color: #ffc107; padding: 5px; text-align: center;"> Hay disponible una nueva versión de GP Premium. <a href="#">Revisar</a></div>	
<input type="checkbox"/> <b>H5P</b>	Te permit
<a href="#">Desactivar</a>   <a href="#">Settings</a>	Versión 1
<input type="checkbox"/> <b>IONOS Performance</b>	IONOS Pe
<a href="#">Activar</a>   <a href="#">Borrar</a>	utilizar es activandc
	Versión 2
<input type="checkbox"/> <b>PDF Poster</b>	You can e
<a href="#">Actualizar</a>   <a href="#">Inscribirse</a>   <a href="#">Desactivar</a>	Versión 2
<input type="checkbox"/> <b>Spectra</b>	<a href="#">Spectra a</a>

Con respecto a los plugins de bloques como spectra, generateblocks, etc trataría de trabajar solo con uno de ellos para evitar posibles incompatibilidades.

## 4. Estado de salud del sitio

Para tener una visual del estado de salud del sitio web nos dirigimos a **Herramientas > Salud del sitio** y en este caso nos encontramos con 2 avisos de seguridad y 4 relacionados con el rendimiento.

### Seguridad:

Deberías eliminar los plugins inactivos

Seguridad



Los plugins amplían la funcionalidad de tu sitio con cosas como formularios de contacto, comercio electrónico y muchas otras. Esto significa que tienen un profundo acceso a tu sitio y, por tanto, es vital mantenerlos actualizados.

Tu sitio tiene 5 plugins esperando ser actualizados.

Tu sitio tiene 1 plugin inactivo. Los plugins inactivos son objetivos tentadores para los atacantes. Si no vas a usar un plugin, deberías plantearte eliminarlo.

[Gestionar tus plugins](#)

[Actualiza tus plugins](#)

[Gestionar los plugins inactivos](#)

---

Deberías eliminar los temas inactivos.

Seguridad



Los temas añaden el aspecto y comportamiento de tu sitio. Es importante tenerlos actualizados, para mantener la coherencia con tu marca y mantener tu sitio seguro.

Tu sitio tiene 1 tema esperando a ser actualizado.

Tu sitio tiene 1 tema inactivo, aparte de Twenty Twenty-Five, el tema por defecto de WordPress, y GeneratePress, tu tema activo. Deberías plantearte eliminar cualquier tema no usado para mejorar la seguridad de tu sitio.

[Gestiona tus temas](#)

### Rendimiento:

Tu sitio está ejecutando una versión antigua de PHP (8.1.32) que debería ser actualizada

Rendimiento



PHP es uno de los lenguajes de programación utilizados para crear WordPress. Las versiones más recientes de PHP reciben actualizaciones de seguridad frecuentes y pueden mejorar el rendimiento de tu sitio. La versión mínima recomendada de PHP es la 8.3.

[Aprende más sobre actualizar PHP](#) ↗

---

Un evento programado ha fallado

Rendimiento



El evento programado, wordfence\_ls\_ntp\_cron, no se ha podido ejecutar. Tu sitio todavía funciona, pero esto puede indicar que las entradas programadas o las actualizaciones automáticas no funcionen como deberían.

## Deberías utilizar una caché de objetos persistente

Rendimiento



Una caché de objetos persistente hace que la base de datos de tu sitio sea más eficiente, lo que da como resultado tiempos de carga más rápidos porque WordPress puede recuperar el contenido y los ajustes de tu sitio mucho más rápidamente.

Tu proveedor de alojamiento puede decirte si la caché de objetos persistente puede activarse en tu sitio.

[Aprende más acerca de la caché de objetos persistente.](#) ↗

## No se puede detectar la presencia de la caché de página

Rendimiento



No se puede detectar el almacenamiento en caché de página debido a un posible problema de solicitud de bucle de retorno. Por favor, verifica que la prueba de solicitud de bucle de retorno es correcta. Error: cURL error 28: Operation timed out after 5001 milliseconds with 0 bytes received (Código: http\_request\_failed)

El almacenamiento en caché de página mejora la velocidad y el rendimiento de tu sitio al guardar y servir páginas estáticas en lugar de llamar a una página cada vez que un usuario la visita.

El almacenamiento en caché de página se detecta buscando un plugin de almacenamiento en caché de la página activo, así como realizando tres peticiones a la página principal y buscando una o más de las siguientes cabeceras de respuesta de almacenamiento en caché del cliente HTTP:

`cache-control`, `expires`, `age`, `last-modified`, `etag`, `x-cache-enabled`, `x-cache-disabled`, `x-srccache-store-status`, `x-srccache-fetch-status`.

[Aprende más sobre la caché de página](#) ↗

Esto sería un desglose de cada aviso, pero en la parte superior de página nos avisa del estado general del sitio:

## Salud del sitio



Bueno

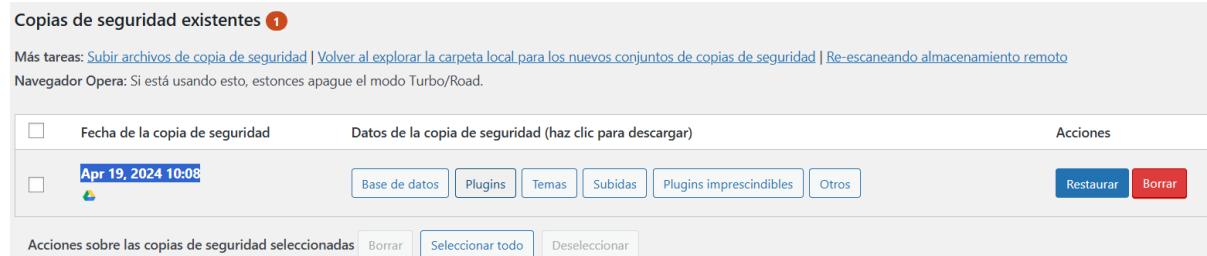
Estado

Información

*Nota: Es importante tener en cuenta en el apartado 'Ajustes>Medios' tener a 0 los tamaños de archivos subidos, esto nos ahorrará mucho espacio en nuestro servidor.*

## 5.Copia de seguridad (UpdraftPlus Backup/Restore)

Al acceder al plugin ‘UpdraftPlus’ nos damos cuenta que no tenemos hecha copia de seguridad del sitio web desde Abril del 2024.



Copias de seguridad existentes 1

Más tareas: [Subir archivos de copia de seguridad](#) | [Volver al explorar la carpeta local para los nuevos conjuntos de copias de seguridad](#) | [Re-escaneando almacenamiento remoto](#)

Navegador Opera: Si está usando esto, estónces apague el modo Turbo/Road.

Fecha de la copia de seguridad	Datos de la copia de seguridad (haz clic para descargar)	Acciones
Apr 19, 2024 10:08 	Base de datos Plugins Temas Subidas Plugins imprescindibles Otros	<a href="#">Restaurar</a> <a href="#">Borrar</a>

Acciones sobre las copias de seguridad seleccionadas [Borrar](#) [Seleccionar todo](#) [Deseleccionar](#)

Hacer copias de seguridad (backups) es una práctica técnica esencial para sitios WordPress, ya que permite restaurar el sitio en caso de hackeos, fallos de servidor, actualizaciones problemáticas o errores humanos. Una copia de seguridad completa incluye archivos y base de datos, garantizando que, ante cualquier incidente, se pueda recuperar la web en minutos minimizando tiempo fuera de servicio y pérdida de datos.

En cuanto a la periodicidad, la recomendación más segura es realizar backups diarios si el sitio recibe cambios o publicaciones frecuentes, como en blogs activos o tiendas online. Si el sitio es estático o se actualiza poco, pueden ser suficientes copias semanales o quincenales. El backup debe ejecutarse siempre antes de grandes modificaciones: actualizaciones, cambios de hosting o instalaciones masivas de plugins/temas.

Como protocolo de seguridad, se debería establecer un calendario automático de backups acorde al uso del sitio, asegurando almacenamiento en una ubicación externa segura y monitoreando regularmente la integridad de las copias para evitar sorpresas negativas si llega el momento de restaurar.

## 6.Accesos :Usuarios y roles.

Tener un número elevado de administradores (en este caso, 7) es contraproducente porque cada cuenta con ese rol tiene acceso total al sitio, incluida la instalación de plugins, edición de código, cambios en configuraciones y gestión de otros usuarios. Si una cuenta es comprometida, el atacante puede tomar control completo y causar daños graves, como robo o borrado de datos, instalación de malware o suplantación de identidad. Se recomienda limitar los administradores solo a usuarios de máxima confianza y experiencia, aplicando el principio de mínimo privilegio: asignar a cada usuario solo los permisos necesarios para su función.

Respecto al 2FA (autenticación en dos factores), tener más de la mitad de las cuentas (19 de 33) sin esta protección incrementa el riesgo de acceso no autorizado por fuerza bruta, phishing o filtraciones de contraseñas, sobre todo en cuentas administrativas. Activar el 2FA

en todos los administradores y usuarios con acceso al backend es esencial para elevar la seguridad y reducir la probabilidad de ataques exitosos. El 2FA añade una barrera adicional que impide el acceso, aunque se robe o filtre la contraseña.

Por último, hay que revisar periódicamente todos los usuarios, eliminar cuentas inactivas o innecesarias, y exigir contraseñas fuertes y únicas para cada usuario. Mantener controles de acceso estrictos es clave para proteger el sitio frente a amenazas internas y externas.

## → Implementación efectiva de 2FA para todos los usuarios

Para implementar 2FA en WordPress de forma efectiva, basta instalar un plugin como WP 2FA o Wordfence Login Security, configurarlo para exigir doble verificación a todos los usuarios y seguir el asistente que guía paso a paso la activación para cada perfil. El usuario define su método (app móvil o correo) y confirma que la verificación funciona correctamente. Esto añade una segunda capa de seguridad y reduce el riesgo de accesos no autorizados.

## → Comentarios de usuarios

Podemos ver un volumen elevado de comentarios pendientes (2.637), ninguno aprobado y solo 2 marcados como spam. Esto indica que la moderación manual está activada y evita que mensajes irrelevantes o peligrosos sean públicos, pero la acumulación puede saturar el sistema y afectar el rendimiento del sitio. Además, la ausencia de comentarios aprobados sugiere que no se ha revisado ni gestionado la participación, lo que dificulta el diálogo real y la reputación del sitio.

Este nivel de comentarios pendientes puede esconder spam, ciberataques y enlaces maliciosos que **afectan el SEO y la seguridad**. Los pasos recomendados incluyen:

- Revisar y depurar la cola actual, aprobando solo comentarios válidos y bloqueando el spam.
- Configurar palabras clave y filtros para enviar automáticamente mensajes sospechosos a spam o papelera.
- Usar un plugin anti-spam como Akismet o Antispam Bee para prevenir acumulaciones futuras y facilitar la gestión automatizada.
- Restringir los comentarios anónimos y exigir datos válidos para reducir el spam automatizado.

Mantener un sistema de comentarios controlado mejora la seguridad, credibilidad y calidad del sitio.

## Acciones

El primer paso es reducir el número de perfiles Administrador, para ello desde el panel de usuarios editamos cada perfil degradando de Administrador a Suscriptor.

Una vez que hemos reducido el número de usuarios con rol de Administrador nos dirigimos al plugin Wordfence y en el apartado de seguridad del acceso configuramos qué roles queremos aplicarle la doble autenticación (2FA).

### 2FA

Roles 2FA				
Administrador	Editor	Author	Contributor	Subscriber
Opcional	Obligatorio	Obligatorio	Obligatorio	Obligatorio

#### Periodo de gracia

 días

Para los perfiles para los que es obligatorio 2FA, los usuarios tendrán este montón de días para configurar 2FA. Si no configuran 2FA durante este periodo resultará en que el usuario perderá el acceso a la cuenta. Este periodo de gracia se aplicará a los nuevos usuarios desde el momento de creación de la cuenta. Para los usuarios existentes, este periodo de gracia se aplicará de manera relativa al momento en que se implemente el requisito. Este periodo de gracia no se aplicará automáticamente a los administradores, y debe activarse manualmente para cada usuario administrador.

#### Avisos 2FA

Envía un correo electrónico a los usuarios con el perfil seleccionado para avisarles del periodo de gracia que tiene para activar 2FA. Selecciona el perfil deseado y, opcionalmente, especifica la URL a enviar en el correo electrónico para configurar 2FA. Si se deja en blanco la URL por defecto lleva al proceso de acceso estándar de WordPress y a la página de identificación en dos factores del plugin Wordfence. Por ejemplo, si usas WooCommerce, introduce la URL relativa de la página de la cuenta. [?](#)

Perfil 2FA	URL 2FA relativa (opcional)
<input type="button" value="Administrator"/>	<input type="text" value="ex: /my-account/"/>
	<input type="button" value="AVISAR"/>

Una vez aplicado la doble autenticación, se enviará un correo al usuario notificando dicho cambio, de hecho si volvemos a la pestaña usuarios:

	Nombre de usuario	Nombre	Correo electrónico	Perfil	Entradas	Estado de 2FA	Último acceso
<input type="checkbox"/>	 anabelgc	—	anabelgc@seguridadlarinco.nada.es	Suscriptor	0	Inactivo (periodo de gracia)	October 21, 2024 11:57 am
<input type="checkbox"/>	 brima	Blanca Ríos Maya	blancariosmaya18@gmail.com	Suscriptor	8	Activado	June 17, 2024 11:15 am
<input type="checkbox"/>	 carlosdues	—	carlosdues@seguridadlarinconada.es	Suscriptor	0	Inactivo (periodo de gracia)	November 20, 2024 8:14 am
<input type="checkbox"/>	 cdila	Owen Díaz	cristinadiazlara2001@gmail.com	Suscriptor	7	Activado	May 13, 2024 8:47 am

Podemos ver como hay usuarios que tenían el 2FA ya activado y otros no lo tenían, estos últimos están en periodo de gracia.

En el apartado **comentarios** habría que revisarlos y hacer una limpieza de los mismos ya que 2664 mensajes sin revisar afectan a la seguridad y el SEO del sitio.

Lo correcto sería revisar los mensajes y tomar acción al respecto, marcándose como spam, rechazando o aprobando el mensaje.

Atendiendo a algunas señales como :

- Correos raros o sin sentido (por ejemplo: "[asdf123@email.com](mailto:asdf123@email.com)"),
- Nombres sospechosos o generados aleatoriamente.
- Comentarios idénticos que parecen estar generados automáticamente
- Enlaces a webs desconocidas

Autor	Comentario
<input type="checkbox"/>  Index Home 0 aprobados <a href="http://gate-io-shinj.cryptoarhome.com">gate-io-shinj.cryptoarhome.com</a> x 72891023@outlook.com 113.16.17.242	Thank you, your article surprised me, there is such an excellent point of view. That learned a lot. <a href="http://gate-io-shinj.cryptoarhome.com">http://gate-io-shinj.cryptoarhome.com</a> <a href="http://gate-io-shinj.cryptoarhome.com">http://gate-io-shinj.cryptoarhome.com</a>
<input type="checkbox"/>  Index Home 0 aprobados <a href="http://gate-box.cryptoarhome.com">gate-box.cryptoarhome.com</a> x 35732676@outlook.com 218.21.88.91	Thank you, your article surprised me, there is such an excellent point of view. That learned a lot.
<input type="checkbox"/>  Index Home 0 aprobados <a href="http://binance-aggregate-trades.cryptoarhome.com">binance-aggregate-trades.cryptoarhome.com</a> x 54298185@outlook.com 171.104.130.176	Thank you, your article surprised me, there is such an excellent point of view. That learned a lot.

Decidimos catalogarlos como Spam. Por otro lado aprovechamos para vaciar los mensajes de spam:

## Comentarios

[Todos \(0\)](#) | [Míos \(0\)](#) | [Pendientes \(0\)](#) | [Aprobados \(0\)](#) | **Spam (192)** | [Pa](#)

[Acciones en lote](#)

[Aplicar](#)

[Todos los tipos de cor](#)

[Acciones en lote](#)

Comentario

[No es spam](#)

Thank you for your s

**Borrar permanentemente**

Para garantizar más seguridad con respecto al registro y creación de los usuarios:

The screenshot shows a standard WordPress login interface. At the top, there are fields for 'Nombre de usuario o correo electrónico' (Username or email address) and 'Contraseña' (Password). Below the password field is a 'reCAPTCHA' verification box labeled 'No soy un robot'. The reCAPTCHA logo features a blue and grey checkmark-like shape. To the right of the checkbox, there is a link to 'Privacidad - Términos' (Privacy - Terms). Below the reCAPTCHA box are two buttons: a white square for 'Recuérdame' (Remember me) and a blue button for 'Acceder' (Access).

## 7. Yoast SEO

Yoast SEO es un plugin para WordPress diseñado para ayudar a optimizar el contenido de un sitio web desde el punto de vista del SEO (posicionamiento en buscadores). Funciona como un asistente que guía en la configuración técnica y de contenido para que los motores de búsqueda entiendan mejor las páginas y las posiciones en resultados orgánicos mejoren.

Entre sus funciones destacan el análisis de palabras clave, la mejora de la legibilidad del contenido, la gestión de meta descripciones, la creación y optimización de sitemaps XML y la configuración de breadcrumbs para facilitar la navegación. Yoast ofrece tanto una versión gratuita, suficiente para la mayoría de sitios, como una versión premium con funcionalidades avanzadas como análisis para múltiples palabras clave, sugerencias de enlaces internos y gestor de redirecciones.

Es el plugin SEO más popular en WordPress, ampliamente valorado por su facilidad de uso y efectividad, ideal tanto para principiantes como para expertos en SEO, por lo cual recomendaría usarlo. A priori no he encontrado incompatibilidades con los plugins ya instalados, sin embargo, dado que algunos plugins de bloques (GenerateBlocks, Spectra) y performance (IONOS Performance) están instalados, siempre conviene hacer pruebas en un entorno de staging por si surgen incompatibilidades menores,

especialmente con funcionalidades avanzadas de análisis o generación dinámica de contenido.

## → Simplificación de plugins

Teniendo en cuenta estos plugins de bloques que tenemos instalados se podría plantear reducir el número de los mismos. Si se busca un equilibrio entre funcionalidad, rendimiento y facilidad de uso, la mejor elección sería **utilizar Spectra como único plugin** de bloques. Spectra ofrece una amplia variedad de bloques visuales, incluyendo galerías y carruseles, por lo que puede cubrir todas las necesidades sin necesidad de añadir más plugins que sobrecarguen el sitio.

Usar solo Spectra simplifica la gestión, reduce posibles conflictos y mantiene ligero el entorno de bloques.

Si se desea un control más detallado y una optimización máxima de peso y rendimiento, se podría combinar GenerateBlocks para la maquetación básica y un plugin especializado en carruseles (como el Bloque de carrusel de diapositivas) para las funciones específicas de slider, pero esta combinación añade complejidad y potenciales incompatibilidades.

### Términos:

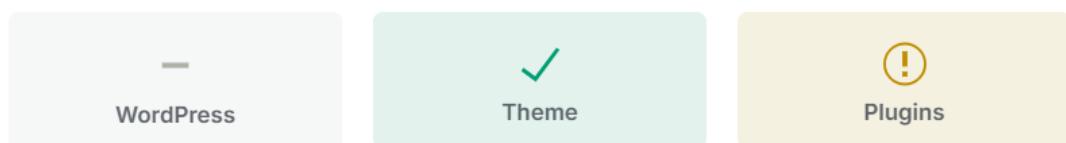
- *Análisis de palabras clave*: Es el proceso de identificar y evaluar las palabras o frases que los usuarios utilizan para buscar contenido relacionado con tu sitio. Yoast SEO analiza si estás utilizando correctamente las palabras clave objetivo en tu contenido para mejorar su posicionamiento en buscadores.
- *Mejora de la legibilidad del contenido*: Esta función evalúa la facilidad de lectura del texto, recomendando ajustes en la estructura, uso de frases cortas, párrafos claros y conectores adecuados para que el contenido sea más atractivo y comprensible tanto para usuarios como para buscadores.
- *Gestión de meta descripciones*: Las meta descripciones son fragmentos de texto que resumen el contenido de una página y que aparecen en los resultados de búsqueda. Este apartado permite crear, personalizar y optimizar esas descripciones para aumentar el porcentaje de clics y atraer al público adecuado.
- *Creación y optimización de sitemaps XML*: Un sitemap XML es un archivo que lista todas las páginas importantes del sitio para que los motores de búsqueda las rastreen y indexen eficientemente. Yoast SEO genera y mantiene actualizado este mapa para mejorar la visibilidad del sitio en buscadores.
- *Configuración de breadcrumbs*: Los breadcrumbs (migas de pan) son elementos de navegación que muestran la ubicación del usuario dentro de la estructura del sitio, facilitando la experiencia de navegación y ayudando a los buscadores a entender la jerarquía del contenido.

## 8.Análisis con WP-Scan

Para poder hacer un diagnóstico general del entorno Wordpress, vamos hacer uso de la herramienta <https://wpscan.com>. Después de realizar el el diagnóstico nos encontramos con que ha detectado vulnerabilidades en la web. En este caso al parecer, hay algún problema con los plugins.

### Your site <https://seguridadlarinconada.es> contains vulnerabilities!

Report generated on October 2, 2025



#### WordPress -

Si bajamos por la web nos indican donde tenemos la incidencia, en el plugin GP-Premium. Si observamos la última línea vemos que nos indica el número de vulnerabilidades, un enlace para ampliar información y una puntuación de severidad.

Plugin: gp-premium ⓘ	
Version	2.4.0
Latest Version	
Last Updated	
1 Vulnerability	<a href="#">GP Premium &lt; 2.4.1 - Reflected Cross-Site Scripting ↗</a>
	<span style="background-color: red; color: white; padding: 2px 5px;">6.1</span> Severity Score

Una vez dentro vemos un informe más detallado de la vulnerabilidad:

## GP Premium < 2.4.1 - Reflected Cross-Site Scripting

### Description

The GP Premium plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the message parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.

### Affects Plugins

---

 gp-premium      Fixed in 2.4.1 ✓

### References

---

CVE	<a href="#">CVE-2024-3469</a>
URL	<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/1a697391-f30d-403f-9046-8fa219a49302">https://www.wordfence.com/threat-intel/vulnerabilities/id/1a697391-f30d-403f-9046-8fa219a49302</a>

### Classification

---

Aquí nos está diciendo que el plugin afectado es GP Premium.

Indica el plugin específico que presenta la vulnerabilidad y la versión afectada (hasta la 2.4.0 incluida).

- Tipo de vulnerabilidad:

Reflected Cross-Site Scripting (XSS)

Es un fallo de seguridad donde el plugin no filtra correctamente los datos de entrada ("message parameter"), lo que permite a un atacante injectar código JavaScript o similar en páginas web que se ejecuta si el usuario realiza una acción (por ejemplo, clicar un enlace malicioso).

El atacante puede preparar un enlace especial que, al ser pulsado por el usuario, desencadena la ejecución de scripts arbitrarios en el navegador, robando información o modificando la página.

*La causa es que el plugin no valida ni escapa correctamente los datos enviados por el usuario. Por lo tanto, la recomendación es **actualizar** el plugin **inmediatamente**.*

Un poco más abajo nos hace una clasificación de dicha vulnerabilidad

## Classification

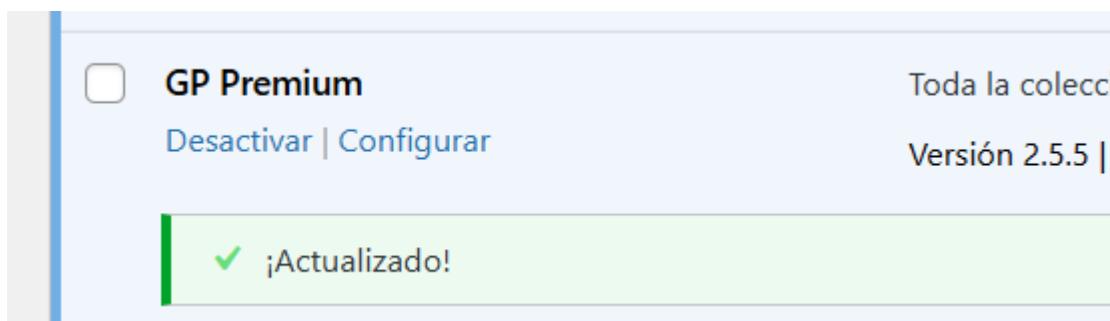
---

Type	XSS
OWASP top 10	A7: Cross-Site Scripting (XSS)
CWE	CWE-79
CVSS	6.1 (medium)

En este caso un A7 atendiendo a la OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web)

- Tipo: XSS
- OWASP top 10: Categoría A7 – Cross-Site Scripting.
- CWE-79: Referencia al tipo de error según el estándar de vulnerabilidades

Por ello en nuestro dashboard de WP nos dirigimos a plugins y actualizamos.



Ahora podemos ver como el sitio es seguro

Your site <https://seguridadlarinconada.es> appears secure!

Report generated on October 2, 2025



## 9. Análisis con Sucuri SiteCheck

Para un análisis de malware y blacklist de la web nos dirigimos a la web <https://sitecheck.sucuri.net> donde insertaremos la url a analizar:

⌚ <https://seguridadlarinconada.es>

Site Issue  
Timeout reached

Site is not Blacklisted  
9 Blacklists checked

Request Review

IP address: 213.158.84.44  
Hosting: Unknown  
Running on: Nginx

CMS: WordPress 6.8.3  
Powered by: Unknown  
[More Details](#)

Minimal Low Security Risk Medium High Critical

**Site Issue Detected**  
<https://seguridadlarinconada.es/inicio/blog/>

[Unable to scan the page. Timeout reached](#)

Ya nos está diciendo la herramienta que el problema lo tenemos en el blog de nuestra web.

---

## Protocolo de actuación WordPress (externas a Wordpress)

- 1. Escaneo de vulnerabilidades y análisis de seguridad (Analizar con WP-SCan.)
- 2. Análisis de malware y blacklist ( Sucuri SiteCheck)
- 3. MIRAR SCRIPT

## Protocolo de actuación WordPress (internas a Wordpress)

- 1. Copia de seguridad antes de cualquier cambio

- Entra en el panel de WordPress.
  - Ve a “Ajustes” → “UpdraftPlus Backup”.
  - Pulsa “Respaldar ahora”.
  - Asegúrate de guardar la copia en la nube o en tu equipo.
- 
- 2. Actualización de WordPress, plugins y temas
  - Ve a “Escritorio” → “Actualizaciones”.
  - Pulsar “Actualizar ahora” si hay nueva versión de WordPress.
  - Sigue con “Plugins”, selecciona todos y pulsa “Actualizar”.
  - Haz lo mismo en “Apariencia” → “Temas”, luego elimina los temas que no utilices.
- 
- 3. Revisión de usuarios y contraseñas
  - Ve a “Usuarios” → “Todos los usuarios”.
  - Cambia el rol de cualquier usuario que no deba ser “Administrador” (elige, por ejemplo, “Suscriptor”).
  - Activa autenticación de dos factores (2FA) si el plugin está disponible.
  - Elimina usuarios que no se utilicen y revisa las contraseñas: que sean fuertes y únicas.
- 
- 4. Auditoría y gestión de plugins
  - Dirígete a “Plugins” → “Plugins instalados”.
  - Elimina cualquier plugin que no estés usando.
  - Si tienes varios que hacen lo mismo (como constructores visuales), quédate solo con uno (recomendado: Spectra).
  - Mantén solo plugins de fuentes seguras y conocidas.
- 
- 5. Moderar los comentarios
  - Entra en “Comentarios”.
  - Marca como spam los que sean sospechosos y elimina los que no sean válidos.
  - Instala y configura un plugin antispam para evitar acumulaciones (ejemplo: Akismet).
- 
- 6. Mejorar el SEO
  - Instala el plugin “Yoast SEO” desde “Plugins” → “Añadir nuevo”.
  - Sigue las sugerencias que aparecen para optimizar títulos, descripciones y el contenido de tus páginas.

- 7. Revisar salud del sitio y avisos
- Accede a “Herramientas” → “Salud del sitio”.
- Revisa los avisos de seguridad o rendimiento.
- Aplica las recomendaciones que se muestran; si tienes dudas, consulta soporte o busca ayuda de un profesional.