

Nombre completo : Milton Alfonso Basante Sanchez

NAO ID : 3218

Fecha : 08/09/2025

Nombre de la trayectoria : Consultor de ciberseguridad

Título del Reto : Protocolos de seguridad con pentesting y criptografía

Informe Técnico – Sprint 2

1. Introducción

El presente informe documenta el desarrollo del **Sprint 2**, cuyo objetivo fue implementar un sitio web en WordPress para la empresa ficticia *ToCupboard*, incluyendo la integración de llamadas a una API y la simulación de una pasarela de pagos, bajo el enfoque del modelo **DevSecOps**.

Se detallan los procesos de instalación, configuración, seguridad aplicada, desarrollo de las funcionalidades solicitadas y la documentación técnica.

2. Desarrollo del Sitio Web en WordPress

2.1 Instalación y Configuración Inicial

- Se desplegó WordPress en un servidor local utilizando **localhost**.
- Se configuró el idioma, base de datos y credenciales de acceso (usuario administrador y contraseña segura).
- Se seleccionó un tema responsive y profesional para representar la identidad visual de *ToCupboard*.

2.1.1 Justificación del Uso de XAMPP

Para el desarrollo del sitio web se utilizó **XAMPP** como entorno de servidor local. La elección de esta herramienta se fundamenta en las siguientes razones:

1. **Entorno Integrado:** XAMPP incluye Apache (servidor web), MySQL/MariaDB (base de datos), PHP y Perl en un solo paquete, lo cual simplifica la instalación y configuración inicial de WordPress.
2. **Facilidad de Uso:** Su interfaz gráfica permite administrar servicios (Apache y MySQL) de manera rápida, lo cual es ideal para entornos de desarrollo y pruebas académicas.

3. **Compatibilidad:** XAMPP es compatible con WordPress y soporta la mayoría de los plugins y temas disponibles en la comunidad.
4. **Entorno Seguro y Controlado:** Al ejecutarse en local, permite experimentar y realizar configuraciones avanzadas sin comprometer datos reales ni exponer servicios a internet.
5. **Portabilidad y Gratuito:** XAMPP es software libre y multiplataforma (Windows, Linux y macOS), lo cual garantiza accesibilidad y facilita su instalación en diferentes equipos.

En conclusión, XAMPP permitió disponer de un **entorno controlado, reproducible y seguro** para la implementación del proyecto ToCupboard, asegurando además una base sólida para la posterior aplicación de prácticas DevSecOps en un servidor de pruebas o de producción.

2.2 Estructura del Sitio

Se incluyeron las siguientes páginas principales:

- **Inicio:** presentación de la marca.
- **Sobre Nosotros:** información de la empresa.
- **Productos/Servicios:** catálogo dinámico gestionado con WooCommerce.
- **Contacto:** formulario para consultas de clientes.

2.3 Seguridad en el Desarrollo

- Actualización de WordPress, tema y plugins.
- Configuración de **HTTPS** mediante certificado SSL.
- Instalación de plugin de seguridad (ej. *Wordfence* o *iThemes Security*).
- Configuración de roles y permisos mínimos necesarios.

Pero en xampp localmente por defecto es HTTP.

3. Llamadas a una API

3.1 Integración de API

Se implementaron ejemplos de llamadas a una API mediante **JavaScript / PHP**, integradas en páginas específicas:

1. **Obtención de datos de productos externos** (ejemplo: consumo de API pública de productos).
2. **Envío de formularios de contacto** con validación hacia un endpoint API.

3.2 Seguridad de las Llamadas

- Uso de HTTPS en la comunicación.
- Implementación de **tokens de autenticación**.
- Validación de entrada de datos antes de enviarlos al endpoint.

4. Simulación de Pasarela de Pagos

4.1 Proceso de Pago

Se utilizó el plugin **WooCommerce**, habilitando pasarelas en modo de pruebas:

- **PayPal Sandbox**
- **Stripe Test Mode**

4.2 Seguridad en el Pago

- Uso de **tokens de pago** en lugar de almacenar datos sensibles.
- Validación de datos antes de procesar la transacción.
- Ejecución en entornos sandbox/test para evitar riesgos reales.

5. Aplicación del Modelo DevSecOps

5.1 Integración DevSecOps

- **Desarrollo:** uso de buenas prácticas seguras en WordPress.
- **Seguridad:** integración de plugins, cifrado SSL y validaciones.
- **Operaciones:** despliegue controlado en entorno local con miras a CI/CD.

5.2 Prácticas Implementadas

- **CI/CD:** integración del repositorio en GitHub para versionado.
- **Pruebas automatizadas:** validación básica con *WPScan* y plugins de testing.
- **Monitoreo:** configuración de alertas y escaneo de vulnerabilidades.

Conclusiones

El desarrollo de este sprint permitió:

- Implementar un sitio funcional en WordPress con diseño seguro.
- Integrar ejemplos de consumo de API con validación de datos.
- Simular un flujo de pagos con prácticas de seguridad modernas.
- Aplicar el enfoque **DevSecOps**, garantizando seguridad desde el inicio hasta el despliegue.

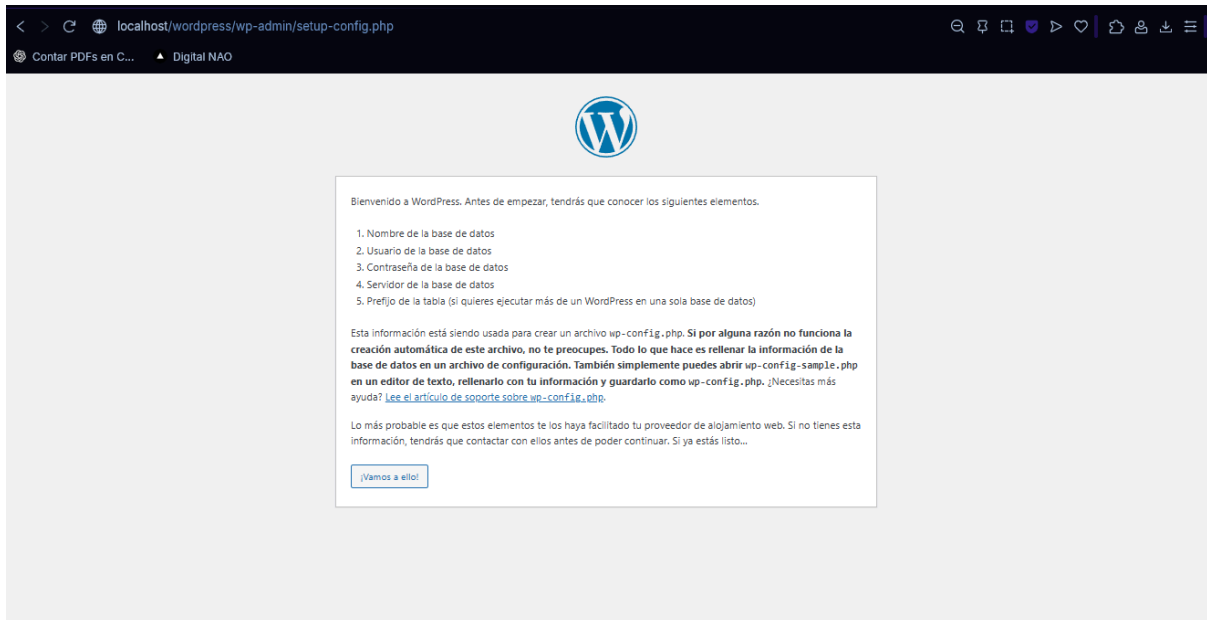
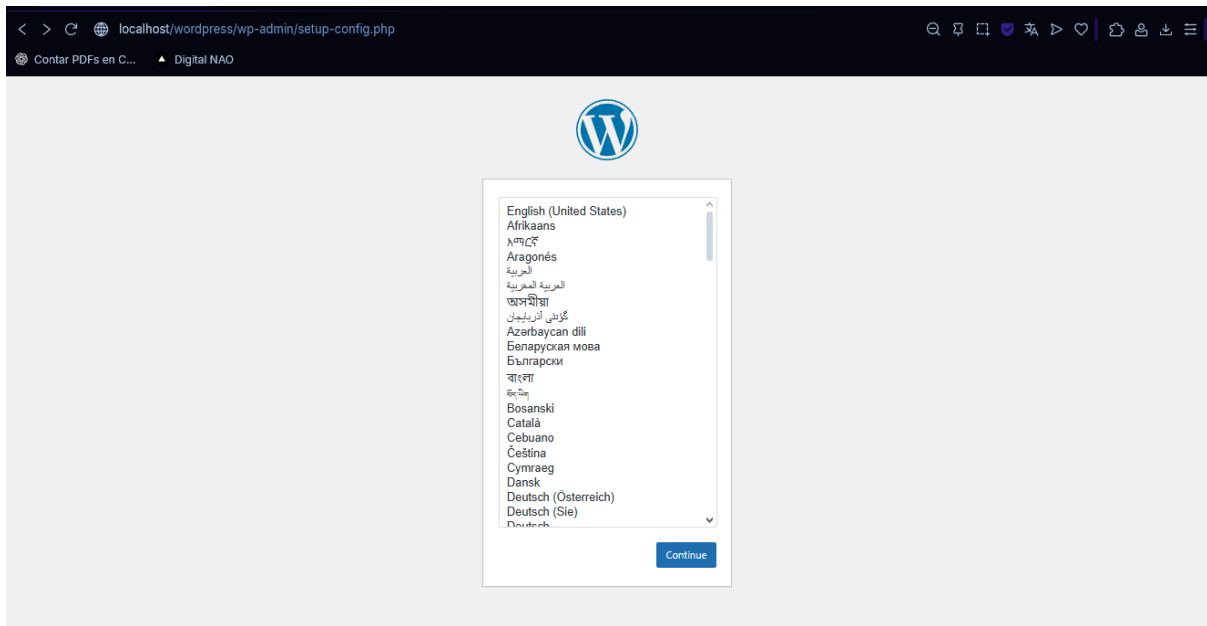
Nota sobre la API y productos mostrados

Durante las pruebas de integración con la API, se observó que los datos obtenidos no correspondían a los productos configurados en WordPress local, sino a información de productos externos.

La causa principal es que:


1. **WordPress en entorno local (localhost)** no expone públicamente su API REST hacia internet.
 - Por ello, al realizar llamadas desde scripts, estas no pueden acceder directamente a los productos creados en WooCommerce en la instalación local.
2. Para efectos de prueba, se utilizó una **API pública** o un endpoint de ejemplo que devuelve productos genéricos.
 - Esto permite validar la integración técnica, aunque los datos no coincidan con los productos propios de la tienda.
3. Para que los productos creados en *ToCupboard* puedan ser consumidos vía API REST, es necesario:
 - Desplegar el sitio en un servidor con dominio o IP accesible.
 - Habilitar la API REST de WooCommerce con credenciales seguras (consumer key y consumer secret).
 - Asegurar las peticiones con HTTPS y tokens de autenticación.

En conclusión, el comportamiento observado es esperado, ya que el desarrollo se encuentra en **entorno local** y no en un dominio público donde la API propia pueda ser consultada desde clientes externos.



localhost/wordpress/wp-admin/setup-config.php

Contar PDFs en C... Digital NAO



A continuación tendrás que introducir los detalles de tu conexión con la base de datos. Si no estás seguro de ellos, contacta con tu proveedor de alojamiento.

Nombre de la base de datos
El nombre de la base de datos que quieres usar con WordPress.

Nombre de usuario
El nombre de usuario de tu base de datos.

Contraseña [Mostrar](#)
La contraseña de tu base de datos.


Servidor de la base de datos
Si localhost no funciona, deberías poder obtener esta información de tu proveedor de alojamiento web.

Prefijo de tabla
Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.

[Enviar](#)

localhost/wordpress/wp-admin/setup-config.php

Contar PDFs en C... Digital NAO



A continuación tendrás que introducir los detalles de tu conexión con la base de datos. Si no estás seguro de ellos, contacta con tu proveedor de alojamiento.

Nombre de la base de datos
El nombre de la base de datos que quieres usar con WordPress.

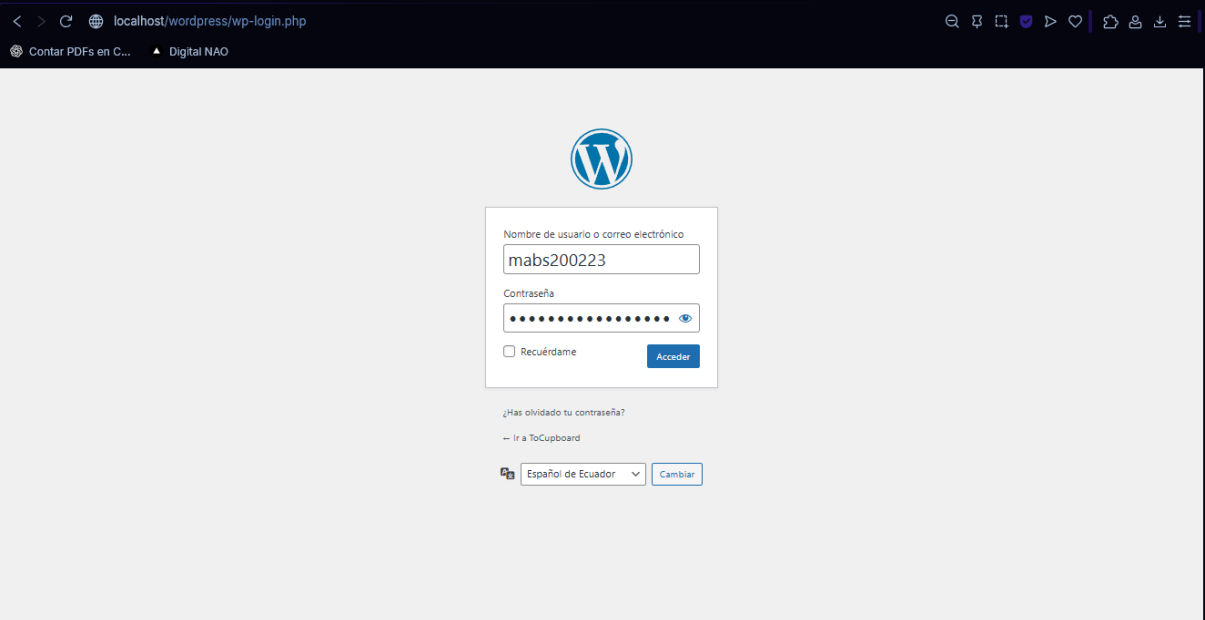
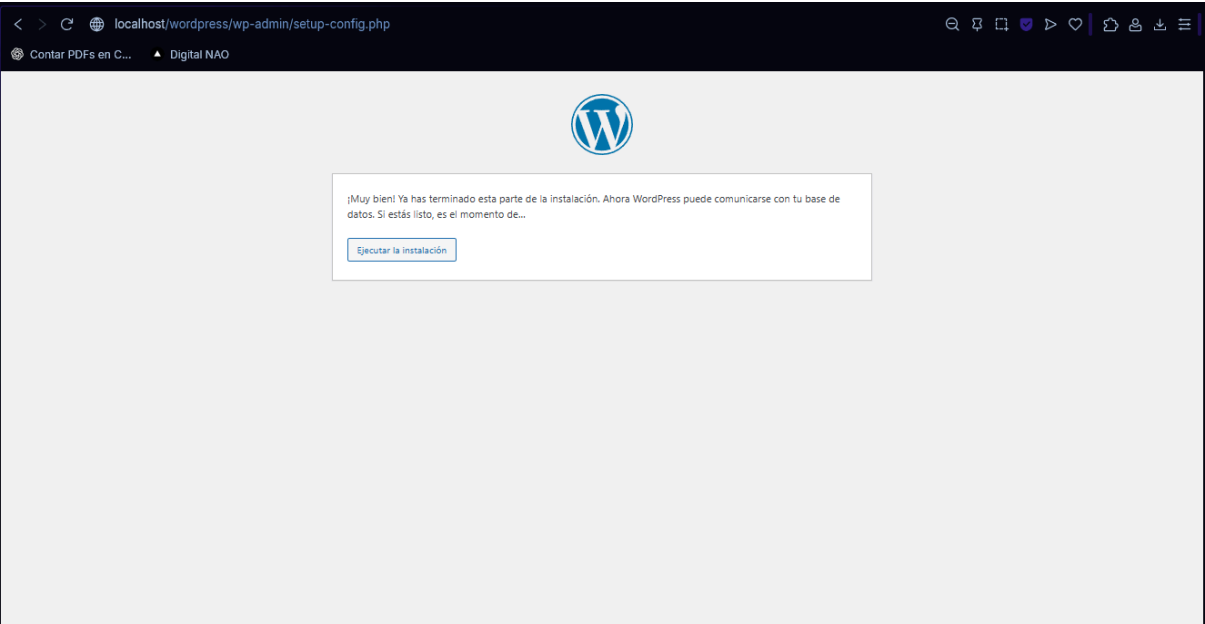
Nombre de usuario
El nombre de usuario de tu base de datos.

Contraseña [Show](#)
La contraseña de tu base de datos.

Servidor de la base de datos
Si localhost no funciona, deberías poder obtener esta información de tu proveedor de alojamiento web.

Prefijo de tabla
Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.

[Enviar](#)



Escritorio < ToCupboard | localhost / 127.0.0.1 / wp-admin/

Contar PDFs en C... | Digital NAO

ToCupboard | 2 | Añadir

Hola, mabs200223

Opciones de pantalla | Ayuda

¡Bienvenido a WordPress!

[Aprende más sobre la versión 6.8.2.](#)

Crea contenido rico con bloques y patrones
Los patrones de bloques son diseños de bloques preconfigurados. Úsalos para inspirarte o crear nuevas páginas en un instante.
[Añadir una nueva página](#)

Personaliza todo tu sitio con temas de bloques
Diseña todo en tu sitio — Desde la cabecera hasta el pie de página. Todo usando bloques y patrones.
[Abrir el editor del sitio](#)

Cambia la apariencia de tu sitio con los estilos
¡Retoca tu sitio o dale un aspecto completamente nuevo! Sé creativo — ¿Qué tal una nueva paleta de color o una nueva fuente?
[Edit styles](#)

Estado de salud del sitio
Aún no hay información... Las pruebas de salud del sitio se ejecutarán automáticamente de forma periódica para obtener información sobre tu sitio. También puedes [visitar ahora la pantalla de salud del sitio](#) para obtener información sobre tu sitio.

Borrador rápido
Título
Contenido
¿Ya estás listo para publicar?

Arrastra aquí las cajas


Añadir plugins

Subir plugin

Resultados de la búsqueda | Destacados | Populares | Recomendados | Favoritos

Buscar plugins | WooCommerce | Palabra clave

10.000 elementos | 1 de 278




WooCommerce
Everything you need to launch an online store in days and keep it growing for years. From your first sale to millions in revenue, Woo is with you.
Por Automattic

★★★★★ (4.594)
7+ millones instalaciones activas

Última actualización: hace 1 semana
✓ Compatible con tu versión de WordPress

[Install Now](#) [Más detalles](#)




Google for WooCommerce
Native integration with Google that allows merchants to easily display their products across Google's network.
Por WooCommerce

★★★★☆ (236)
900.000+ instalaciones activas

Última actualización: hace 3 días
✓ Compatible con tu versión de WordPress

[Install Now](#) [Más detalles](#)




WooCommerce PayPal Payments
PayPal's latest payment processing solution. Accept PayPal, Pay Later, credit/debit cards, alternative digital wallets and bank accounts.
Por WooCommerce

★★★★☆ (466)
700.000+ instalaciones activas


Última actualización: hace 2 días
✓ Compatible con tu versión de WordPress

[Install Now](#) [Más detalles](#)




WooCommerce Stripe Payment Gateway

[Install Now](#) [Más detalles](#)



WooPayments: Integrated WooCommerce

[Install Now](#) [Más detalles](#)



MailPoet - Newsletters, Email

[Install Now](#) [Más detalles](#)

localhost/wordpress/wp-admin/plugin-install.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

Hola, mabs200223


Añadir plugins

Subir plugin

Resultados de la búsqueda Destacados Populares Recomendados Favoritos

Buscar plugins WooCommerce Palabra clave

10.000 elementos 1 de 278



WooCommerce

Everything you need to launch an online store in days and keep it growing for years. From your first sale to millions in revenue, Woo is with you.

Por Automattic

★★★★★ (4.594)


Última actualización: hace 1 semana

7+ millones instalaciones activas

Compatible con tu versión de WordPress

Instalando...

Más detalles



Google for WooCommerce

Native integration with Google that allows merchants to easily display their products across Google's network.

Por WooCommerce

★★★★☆ (236)

Última actualización: hace 3 días

900.000+ instalaciones activas

Compatible con tu versión de WordPress


Install Now

Más detalles

Additional plugins are required

WooCommerce

Más detalles



WooCommerce PayPal Payments

PayPal's latest payment processing solution. Accept PayPal, Pay Later, credit/debit cards, alternative digital wallets and bank accounts.

Por WooCommerce

★★★★☆ (466)

Última actualización: hace 2 días

700.000+ instalaciones activas

Compatible con tu versión de WordPress


Install Now

Más detalles

Additional plugins are required

WooCommerce


Más detalles



WooCommerce Stripe Payment Gateway

Install Now


Más detalles



WooPayments: Integrated WooCommerce

Install Now

Más detalles



MailPoet - Newsletters, Email

Install Now

Más detalles

localhost/wordpress/wp-admin/plugin-install.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

Hola, mabs200223


Añadir plugins

Subir plugin

Resultados de la búsqueda Destacados Populares Recomendados Favoritos

Buscar plugins WooCommerce Palabra clave

10.000 elementos 1 de 278



WooCommerce

Everything you need to launch an online store in days and keep it growing for years. From your first sale to millions in revenue, Woo is with you.

Por Automattic

★★★★★ (4.594)


Última actualización: hace 1 semana

7+ millones instalaciones activas

Compatible con tu versión de WordPress

Activate

Más detalles



Google for WooCommerce

Native integration with Google that allows merchants to easily display their products across Google's network.

Por WooCommerce

★★★★☆ (236)

Última actualización: hace 3 días

900.000+ instalaciones activas

Compatible con tu versión de WordPress


Install Now

Más detalles

Additional plugins are required

WooCommerce

Más detalles



WooCommerce PayPal Payments

PayPal's latest payment processing solution. Accept PayPal, Pay Later, credit/debit cards, alternative digital wallets and bank accounts.

Por WooCommerce

★★★★☆ (466)

Última actualización: hace 2 días

700.000+ instalaciones activas

Compatible con tu versión de WordPress


Install Now

Más detalles

Additional plugins are required

WooCommerce


Más detalles



WooCommerce Stripe Payment Gateway

Install Now


Más detalles



WooPayments: Integrated WooCommerce

Install Now

Más detalles



MailPoet - Newsletters, Email


Install Now

Más detalles

localhost/wordpress/wp-admin/admin.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

woo



¡Te damos la bienvenida a Woo!

¡Estamos encantados de tenerte con nosotros! Te guiaremos por el proceso de configuración, pero antes, contesta unas preguntas para disfrutar de una experiencia totalmente adaptada a ti.

Configurar mi tienda

Saltar la configuración guiada

woo

Cuéntanos algo más sobre tu tienda

Usaremos esta información para ayudarte a configurar pagos, envíos e impuestos, así como para recomendarte el mejor tema para tu tienda.

PONLE UN NOMBRE A TU TIENDA

ToCupboard

(No te preocupes — siempre puedes cambiarlo más adelante!)

¿QUÉ TIPO DE PRODUCTOS O SERVICIOS TIENES PENSADO VENDER?

Alimentación y bebidas

¿DÓNDE ESTÁ UBICADA TU TIENDA? *

Ecuador — Guayas

YOUR EMAIL ADDRESS


mbasante319@gmail.com

☐ Opt-in to receive tips, discounts, and recommendations from the Woo team directly in your inbox.

Seguir

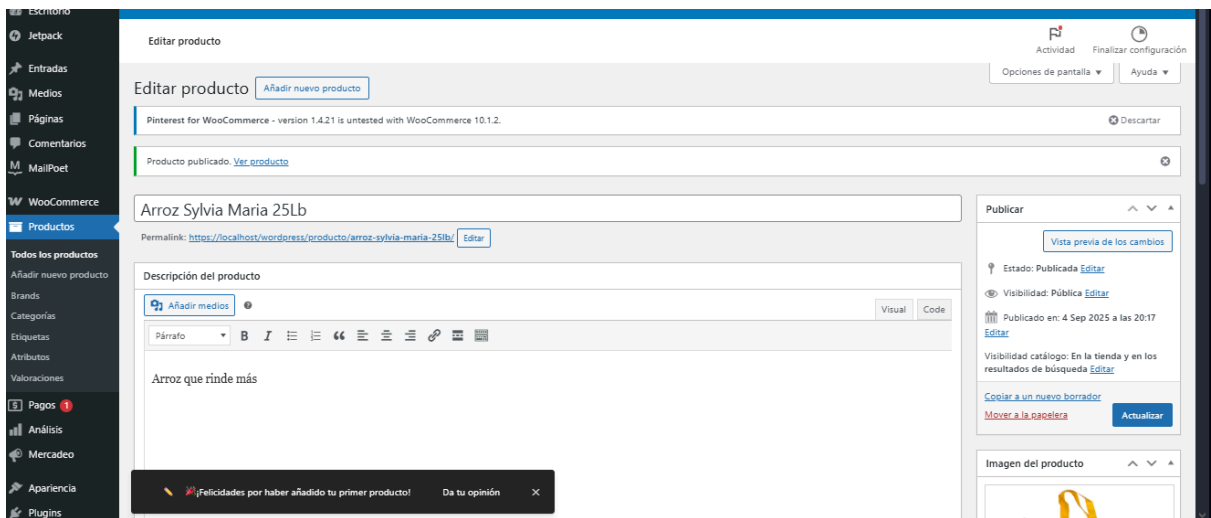
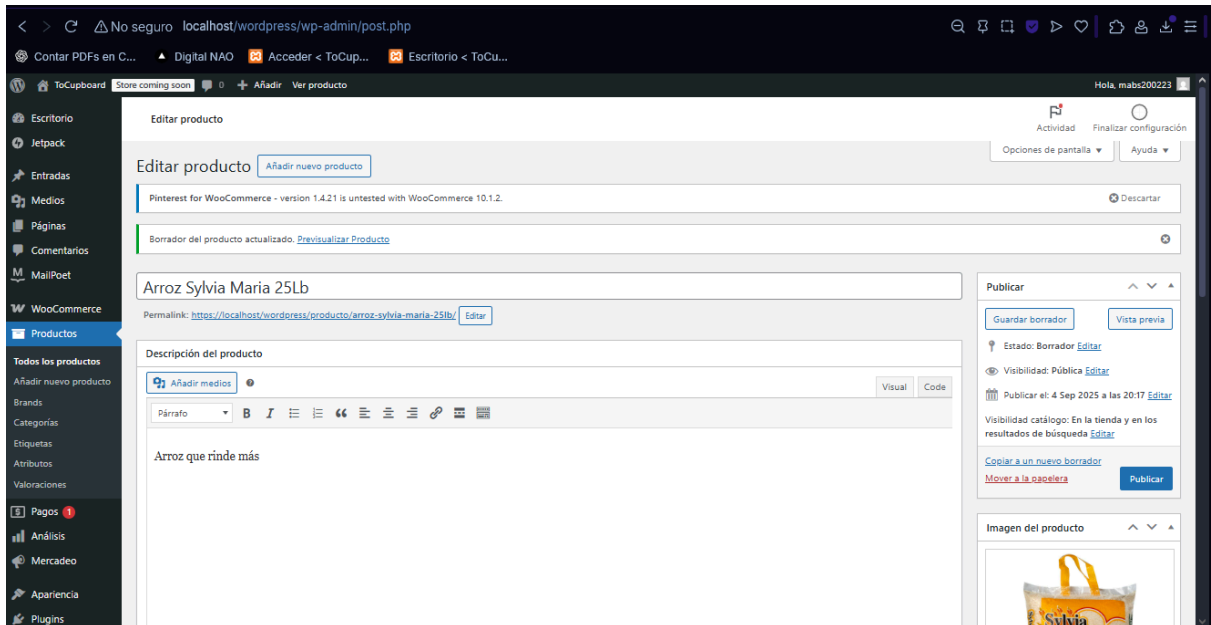
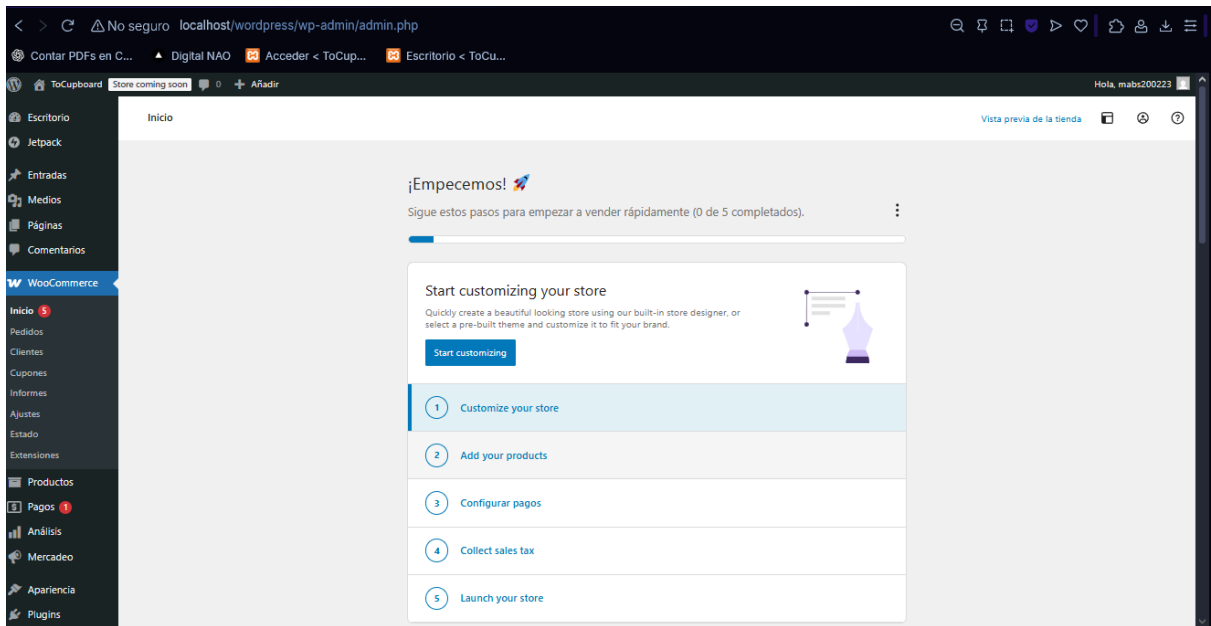
localhost/wordpress/wp-admin/admin.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...



¡Woo! Pongamos en marcha tus características

#CuriosidadesWoo: Did you know that Woo was founded by two South Africans and a Norwegian? Here are three alternative ways to say "store" in those countries – Winkél, ivenkile, and butikk.



localhost/wordpress/producto/frejol-canario-la-pastora-500g

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

ToCupboard Store coming soon Editar el sitio 0 + Añadir Editar producto

Hola, mabs200223

ToCupboard

Carrito Finalizar compra Mi cuenta Página de ejemplo Tienda

Inicio / Granos y Pastas / Fréjol Canario La Pastora 500g

Fréjol Canario La Pastora 500g

\$1,95

Rico en hierro 22% Rico en Fibra y Proteína Calidad Premium Aporta magnesio, potasio, zinc, calcio y fósforo Contenido: 500g

1

Añadir al carrito

Category: [Granos y Pastas](#) Tag: [Granos](#)

This page is in "Coming soon" mode and is only visible to you and those who have permission. To make it public to everyone, [change visibility settings](#)

Productos < ToCupboard Cebolla – ToCupboard Busqueda | Frecuento.co pimienta - Buscar con Go

localhost/wordpress/wp-admin/edit.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

ToCupboard Store coming soon 0 + Añadir Ver productos

Hola, mabs200223

Escritorio Jetpack Entradas Medios Páginas Comentarios MailPoet WooCommerce

Productos







Todos los productos Añadir nuevo producto Brands Categorías Etiquetas Atributos Valoraciones Pagos Análisis Mercadeo Apariencia Plugins

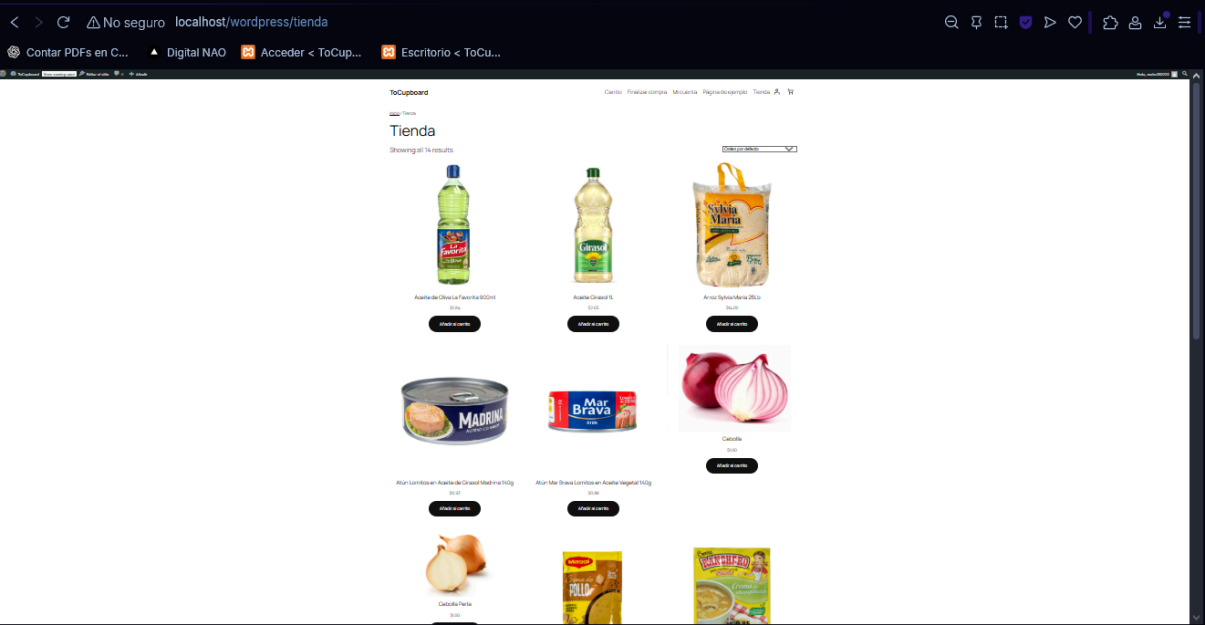
Productos

Añadir nuevo producto Importar Exportar

Todos (14) | Publicados (14) | Ordenar

Acciones en lote Aplicar Elige una categoría Filtrar por tipo de producto Filtrar por estado de invent Filter by brand Filtrar 14 elementos


<input type="checkbox"/>	Nombre	SKU	Inventario	Precio	Categorías	Etiquetas	Brands	Fecha
<input type="checkbox"/>	 Pimiento verde	–	En existencia	\$1,00	Verduras	Verduras	–	Publicada 06/09/2025 a las 10:36
<input type="checkbox"/>	 Cebolla Perla	–	En existencia	\$1,00	Verduras	Verduras	–	Publicada 06/09/2025 a las 10:30
<input type="checkbox"/>	 Cebolla	–	En existencia	\$1,00	Verduras	Verduras	–	Publicada 06/09/2025 a las 10:23
<input type="checkbox"/>	 Crema de Pollo Maggi 65 g ID: 92 Editar Edición rápida Enviar a la Papelera View Duplicar	–	En existencia	\$1,10	Sopas	Crema, Sopas	–	Publicada 06/09/2025 a las 09:57
<input type="checkbox"/>	 Sopa de Pollo Maggi con Arroz 54 g	–	En existencia	\$0,89	Sopas	Sopas	–	Publicada 06/09/2025 a las 09:52
<input type="checkbox"/>	 Crema Ranchero de Champiñones 70g	–	En existencia	\$1,10	Sopas	Sopas	–	Publicada 06/09/2025 a las 09:46



ToCupboard

Carrito Finalizar compra Mi cuenta Página de ejemplo Tienda

Carrito

PRODUCTO	TOTAL	TOTAL DEL CARRITO
 <p>Fréjol Rojo Facundo 140g \$0,98 Fréjoles rojos enlatados Ideal para acompañar el arroz, preparar tacos o lo que quieras No te podrás...</p> <div><div>-</div><div>1</div><div>+</div></div> <p>Eliminar artículo</p>	\$0,98	<div>Add coupons</div> <div>Free shippingGRATIS</div> <div>Estimated total \$0,98</div> <div>Proceder al pago</div>

Dirección de envío

Introduce la dirección donde quieres que se entregue tu pedido.

Pais/Región

Ecuador

Nombre

Milton

Apellidos

Basante

Dirección

Aurora

+ Add apartamento, habitación, etc.

Ciudad

Guayaquil

Estado

Guayas


Código postal

09694

Teléfono (opcional)

Por favor, introduce un código postal válido

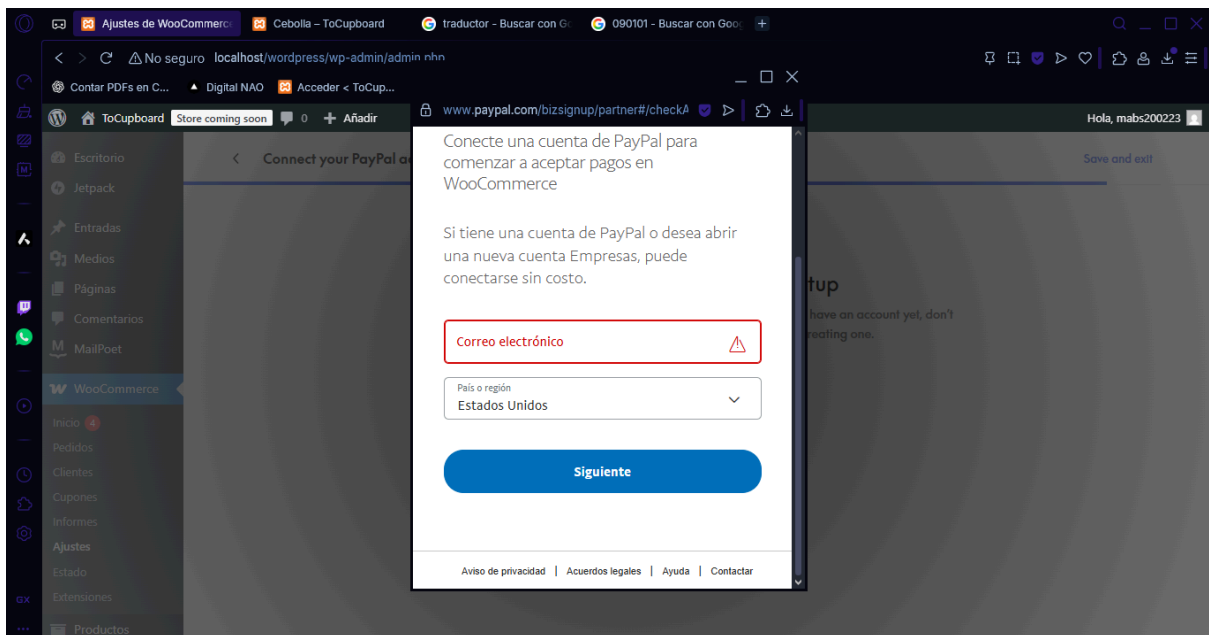
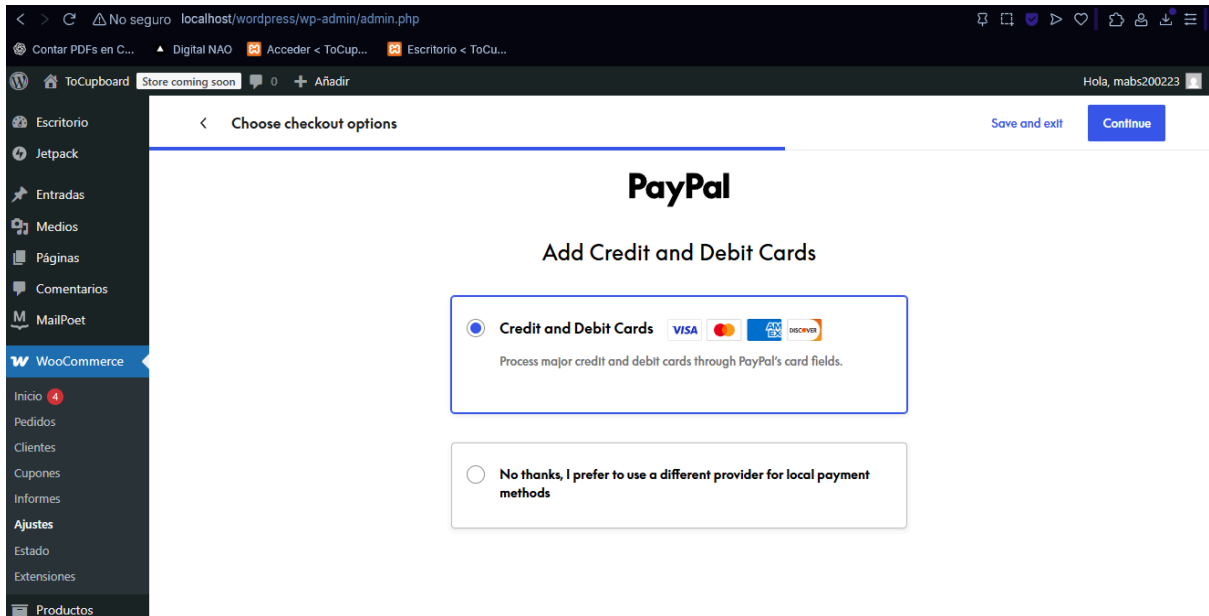
Resumen del pedido

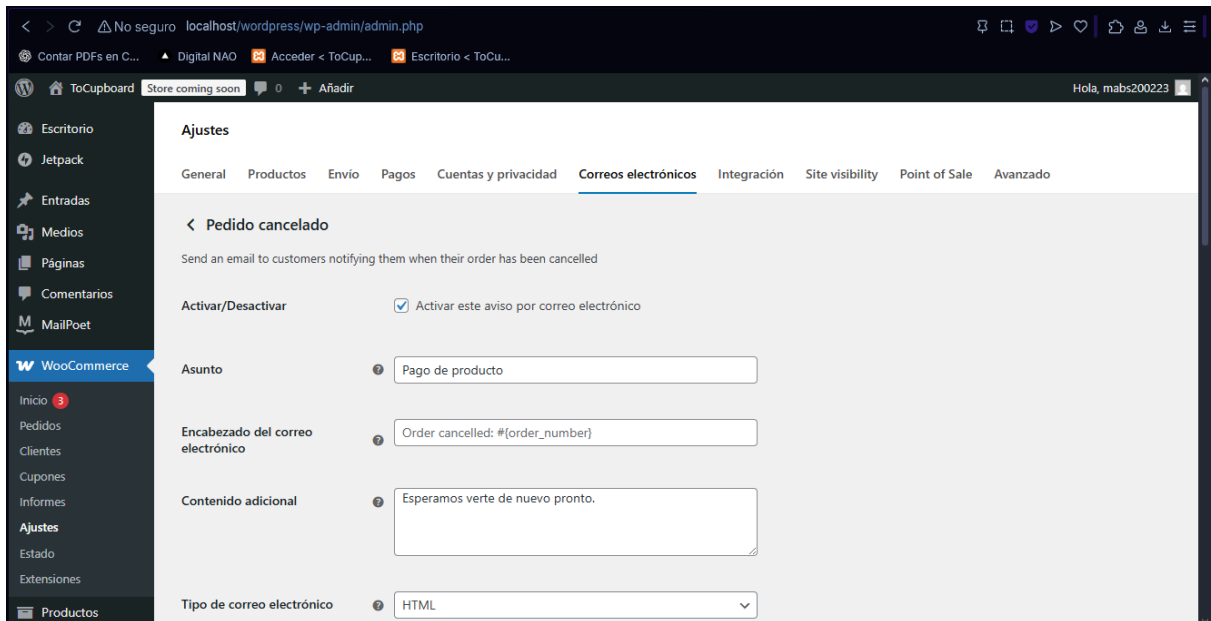
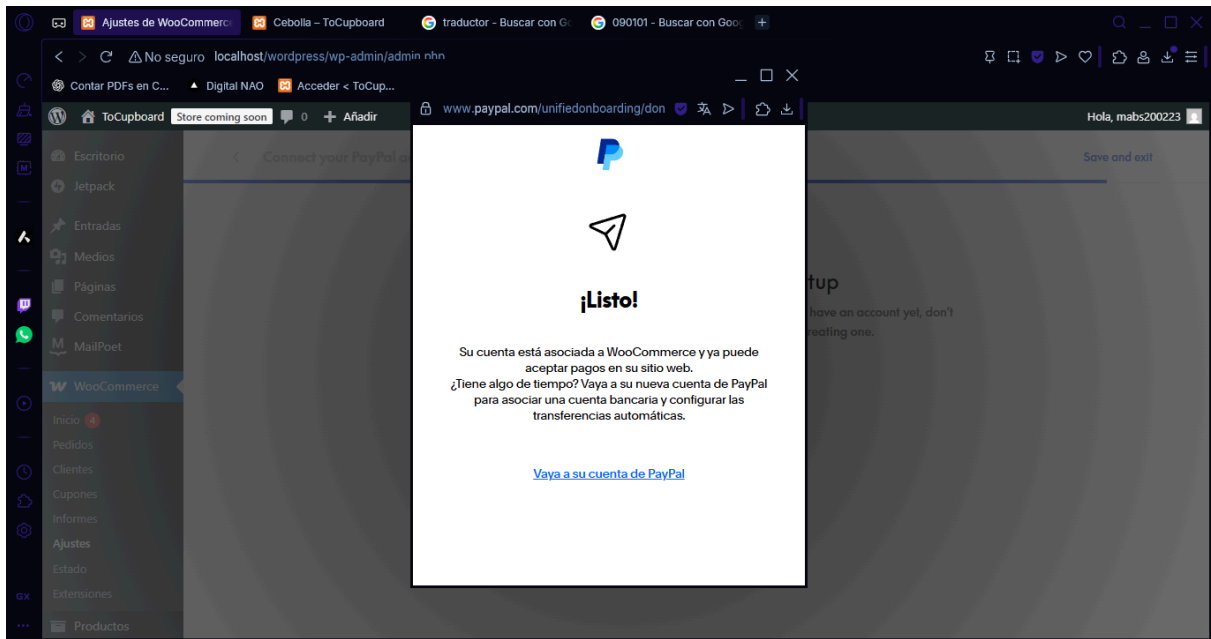
<div>1</div> <div></div> <div>Fréjol Rojo Facundo 140g \$0,98 Fréjoles rojos enlatados Ideal para acompañar el arroz, preparar tacos o lo que quieras No te podrás...</div>	<div>Add coupons</div> <div>Subtotal\$0,98</div> <div>Free shippingGRATIS</div> <div>Total \$0,98</div>
--	---

Código postal

09694

! Por favor, introduce un código postal válido





localhost/wordpress/wp-admin/plugin-install.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

ToCupboard Store coming soon 0 Añadir Hola, mabs200223

Escritorio Jetpack Entradas Medios Páginas Comentarios MailPoet WooCommerce Productos Pagos Análisis Mercadeo Astra Apariencia **Plugins**


Añadir plugins

Subir plugin

Resultados de la búsqueda Destacados Populares Recomendados Favoritos Para Astra-Woo WooCommerce Marketplace

Buscar plugins Wordfence Security Palabra clave

318 elementos 1 de 9



Wordfence Security – Firewall, Malware Scan, and Login Security


Firewall, Malware Scanner, Two Factor Auth, and Comprehensive Security Features, powered by our 24-hour team. Make security a priority with Wordfence.

Por Mark Maunder

★★★★★ (4,661) Última actualización: hace 2 semanas

5+ millones instalaciones activas ☒ Compatible con tu versión de WordPress

Install Now Más detalles



Really Simple Security – Simple and Performant Security (formerly Really Simple SSL)

Easily improve site security with Protección de WordPress, Two-Factor Authentication (2FA), Protección de Inicio de Sesión, Detección de vulnerabilidades and SSL certificate.

Por Really Simple Plugins

★★★★★ (8,751) Última actualización: hace 3 días

4+ millones instalaciones activas ☒ Compatible con tu versión de WordPress

Install Now Más detalles

localhost/wordpress/wp-admin/admin.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

ToCupboard Store coming soon 0 Añadir Hola, mabs200223

Escritorio Jetpack Entradas Medios Páginas Comentarios MailPoet WooCommerce Productos Pagos Análisis Mercadeo Astra Apariencia Plugins

I feel the room swayin'

¿Quieres que Wordfence se mantenga actualizado automáticamente? ☒ Sí, activar la actualización automática. ☐ No, gracias.

Escritorio de Wordfence

Aprende más sobre el escritorio

Protección de Wordfence activada

64%

Cortafuegos

El WAF está actualmente en modo de aprendizaje

[Gestionar el cortafuegos](#)

60%

Analizar

Detección de problemas de seguridad

[Gestionar la exploración](#)

La protección Premium está desactivada

Como usuario gratuito de Wordfence, actualmente estás utilizando la versión de la comunidad del feed de defensa contra amenazas. Los usuarios premium están protegidos por reglas de cortafuegos y firmas de malware adicionales. Actualiza hoy a Premium para mejorar tu protección.

[ACTUALIZAR A LA VERSIÓN PREMIUM](#)

[APRENDE MÁS](#)

Estado de Wordfence Central

localhost/wordpress/wp-admin/admin.php

Contar PDFs en C... Digital NAO Acceder < ToCup... Escritorio < ToCu...

ToCupboard Store coming soon 0 + Añadir Hola, mabs200223

[Volver a Cortafuegos](#) [RESTAURAR AJUSTES POR DEFECTO](#) [CANCELAR CAMBIOS](#) [GUARDAR CAMBIOS](#)

¿Quieres que Wordfence se mantenga actualizado automáticamente? [Sí, activar la actualización automática.](#) | [No, gracias.](#)

Opciones del cortafuegos

Más información sobre el cortafuegos

<div>55%</div> Cortafuegos de la aplicación web Actualmente en el modo de aprendizaje	<div>70%</div> Reglas del cortafuegos:Comunidad Actualmente en el modo de aprendizaje	<div>0%</div> Lista de bloqueos de IPs en tiempo real:Desactivado Solicitudes de bloqueo desde IPs malintencionadas conocidas	<div>100%</div> Protección contra ataques de fuerza bruta Detiene los ataques de adivinación de contraseñas
---	---	---	---

Opciones de cortafuegos básico

Estado del cortafuegos de la aplicación web	Nivel de protección	Lista de bloqueo de IP en tiempo real
--	----------------------------	--

plugins

Este equipo > Disco local (C:) > xampp > htdocs > wordpress > wp-content > plugins > Buscar en plugins

Nuevo > Ordenar > Ver > Detalles

Nombre	Fecha de modificación	Tipo	Tamaño
akismet	4/9/2025 19:54	Carpeta de archivos	
google-listings-and-ads	4/9/2025 20:13	Carpeta de archivos	
jetpack	4/9/2025 20:13	Carpeta de archivos	
mailpoet	4/9/2025 20:13	Carpeta de archivos	
pinterest-for-woocommerce	4/9/2025 20:12	Carpeta de archivos	
woocommerce	4/9/2025 20:06	Carpeta de archivos	
woocommerce-gateway-stripe	6/9/2025 10:53	Carpeta de archivos	
woocommerce-paypal-payments	4/9/2025 20:13	Carpeta de archivos	
wordfence	7/9/2025 10:32	Carpeta de archivos	
hello	6/3/2025 0:18	Archivo de origen ...	3 KB
index	5/6/2014 15:59	Archivo de origen ...	1 KB
tocupboard-api	7/9/2025 11:21	Carpeta de archivos	

12 elementos | 1 elemento seleccionado

