**Forma

El contenido generado por IA puede ser incorrecto.**

**Instituto Superior Universitario Espíritu Santo**

**Carrera**

Ciberseguridad

**Trayectoria:**

Consultor de ciberseguridad | TES Ago25

**Reto N.º 2:**

-Protocolos de seguridad con pentesting y criptografía-

**Autor/es:**

María de los Angeles Torres Cruz

**NAO ID:**

3297

**Tema:**

“Modelo DevSecOps.”

Contenido

[Avance final del Proyecto - Implementación de un E-commerce con DevSecOps para ToCupboard 4](#_Toc209557340)

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.**DETALLE DE LA RETROALIMENTACION DE EXPERTO**

Yo **Torres Cruz María De Los Angeles** se me acusa sobre la utilización de IA la cual es totalmente falso, se me culpa sin preguntar como he logrado este proyecto. Lo que hice fue instalar WordPress en mi computadora un localhost, en ninguna parte de las indicaciones detalla que esto seria una pagina publica, el trasfondo de todo esto es que asumieron que yo hice utilización de IA al 100%, ya que no pueden acceder a la web por el motivo que tengo todo instalado en mi computadora y **NO HAY DE MANERA ALGUNA QUE CHAT GPT O CUALQUIER OTRA HERRAMIENTA DE INTELIGENCIA ARTIFICIAL PUEDA CREAR UNA IMAGEN DE TODAS LAS CAPTURAS DE PANTALLAS QUE HE AGREGADO EN MI TRABAJO. QUIEN SABE DEL USO DE IA VA A SABER QUE NO HAY MANERA DE HACERLO, ESAS CAPTURAS SON LEGITIMAMENTE MIAS**. En vista que han tenido ustedes problemas con revisar mi trabajo repito no a estado de mi lado yo he tenido WordPress instalado, pero nunca me han pedido alguna prueba más, sin embargo, me he tomado la molestia de crear rehacer la web de manera publica para que puedan revisarlo y por favor espero que de esta manera ya puedan constatar finalmente que yo he desarrollado todo lo que me han solicitado hasta ahora. Y así continuar mi proceso de certificación.

He visto trabajos de mis compañeros donde no tienen una pagina web publica y aun les han calificado con un A2 la cual me parece totalmente injusto lo que está pasando con mi caso, necesito respuestas, esta certificación es sumamente importante y no me quiero quedar fuera no exijo que se me certifique con un puntaje alto solamente deseo pasar la certificación. Muchas gracias por su atención debida.

Link de la página web publica: <https://digitalnao.shop/>

Repositorio: [torrescruzmariadelosangeles20-afk/proyectocertificacion.github.io: Certificacion](https://github.com/torrescruzmariadelosangeles20-afk/proyectocertificacion.github.io)

Respaldo sobre la creación pagina web publica: [Respaldos web digitalneo.shop MARIA TORRES .pdf](file:///C:\Users\angel\Downloads\Respaldos%20web%20digitalneo.shop%20MARIA%20TORRES%20.pdf)

# Avance final del Proyecto - Implementación de un E-commerce con DevSecOps para ToCupboard

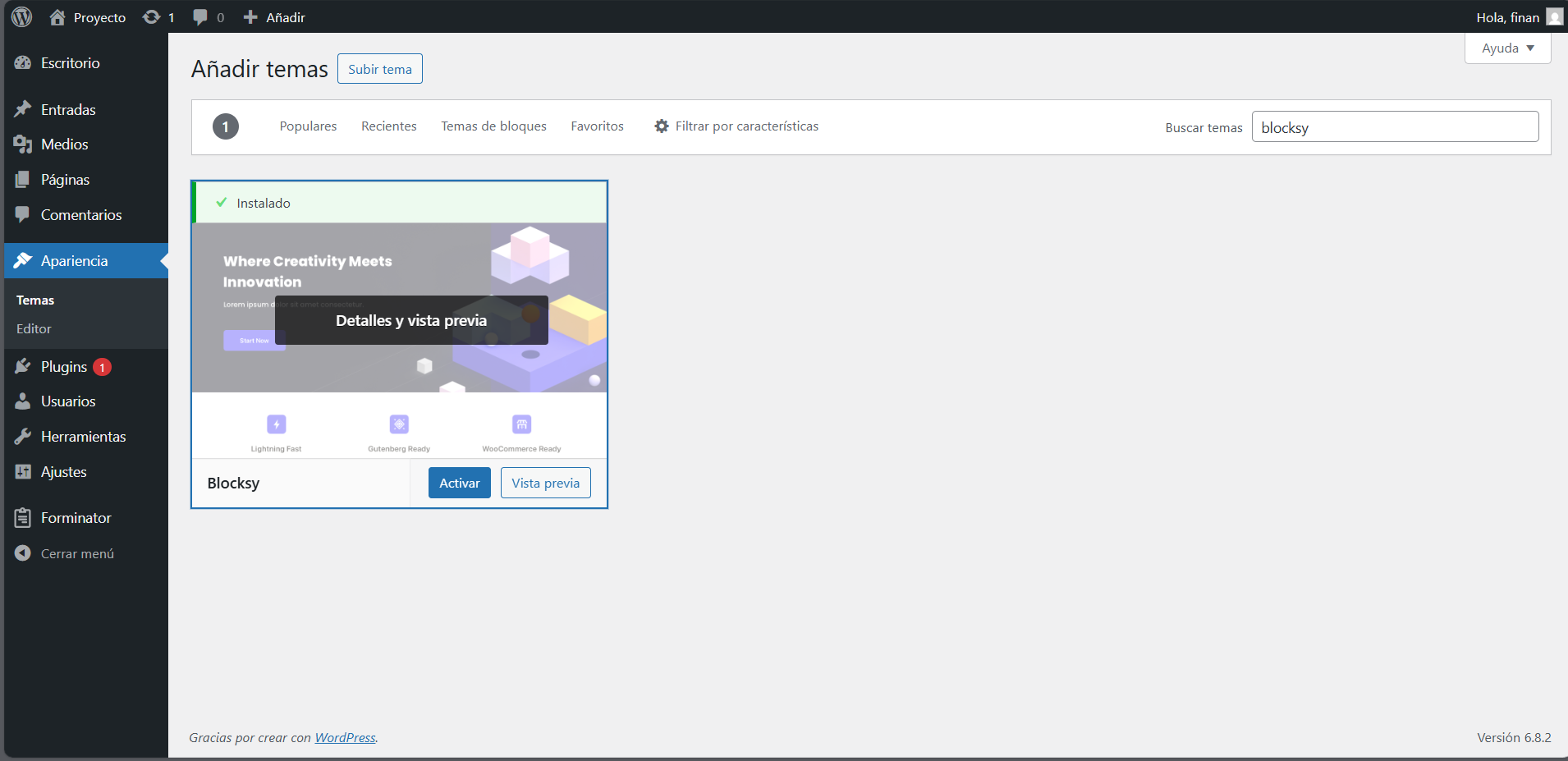
En este informe detalla la implementación del segundo avance del proyecto, que consiste en el desarrollo de un sitio web e-commerce para ToCupboard utilizando WordPress. El proyecto se ha enfocado en la aplicación práctica del modelo DevSecOps, integrando la seguridad en cada etapa del desarrollo. Se ha implementado la integración con una API y una simulación de una pasarela de pagos, siguiendo las mejores prácticas de seguridad.

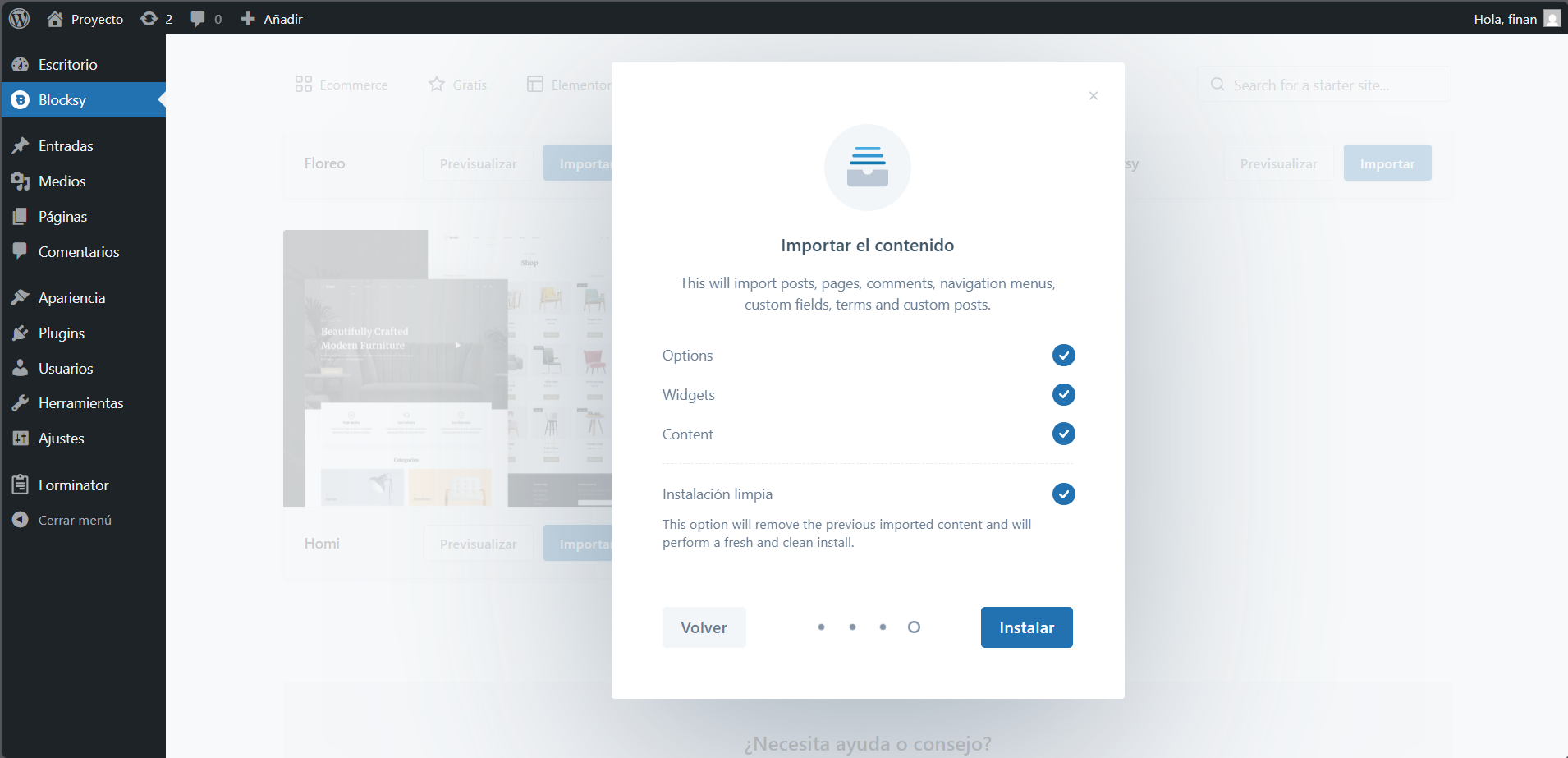
* **Sitio web en Wordpress:**

Para la creación de nuestro sitio web de e-commerce realizamos los siguientes pasos

1. En WordPress hay un apartado de apariencia- temas, descargamos Blocksy esto nos permitirá crear páginas y estilos para nuestra página web a continuación vemos el proceso de instalación:

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.



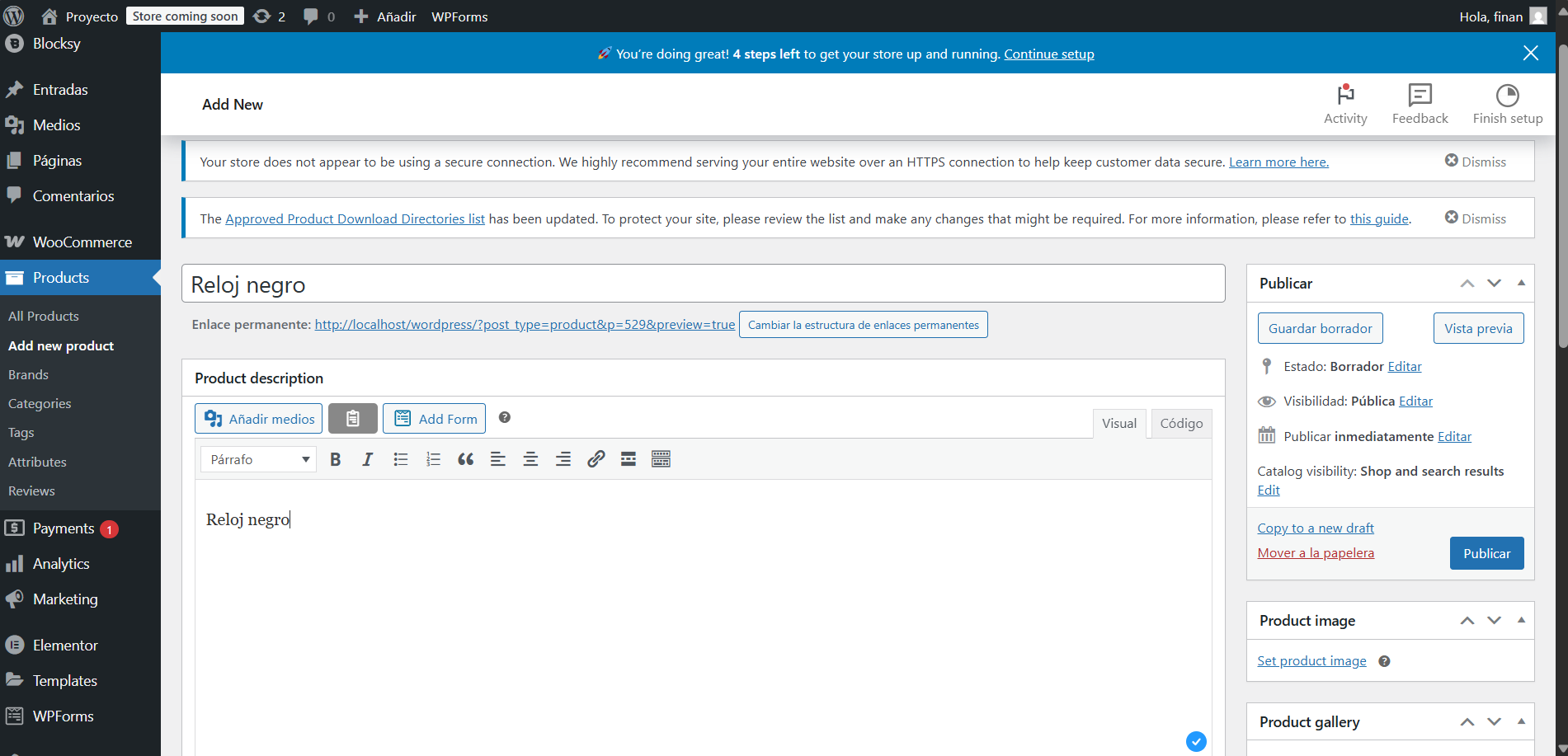
2. Gracias a Elementor pudimos crear nuestra pagina

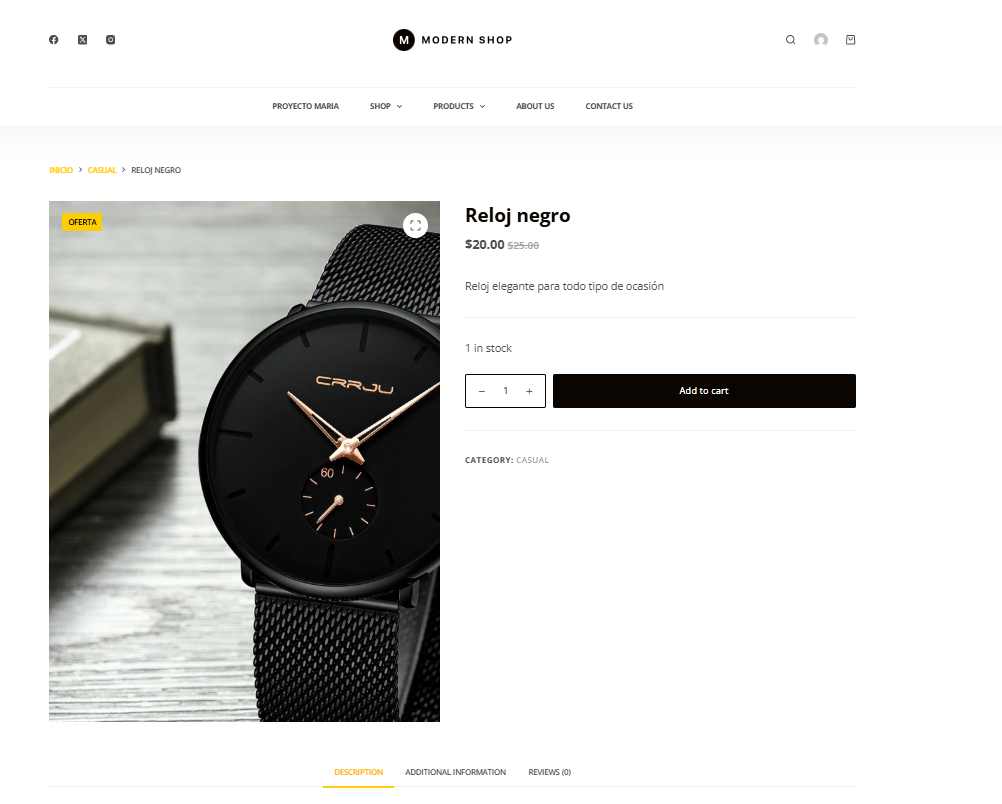
Sitio web, Mapa

El contenido generado por IA puede ser incorrecto.

3. Configuramos los productos que queramos añadir a nuestra tienda

Ejemplo aquí podemos ver la configuración para promocionar un producto en este caso “Un reloj negro” y así se puede configurar con demás productos dependiendo las necesidades del usuario y el estilo de la página.

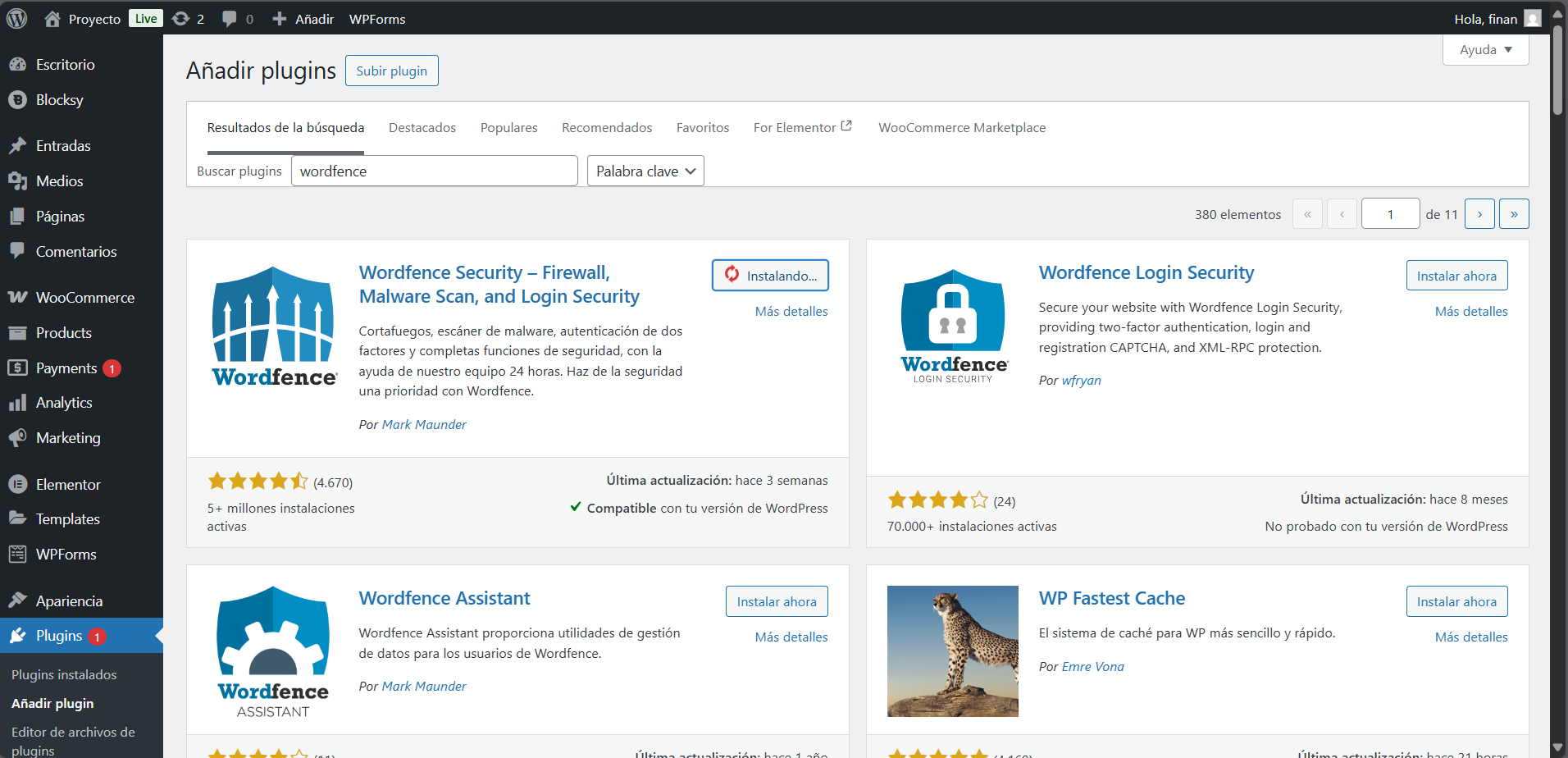




4. Nuestra página debe estar en tipo Live es sumamente importante, tenemos una página sumamente sencilla se pueden agregar muchísimas más cosas, pero este no es el caso así que continuamos con el desarrollo de este proyecto.

Tenemos que agregar un plugin de seguridad para Wordpress en este caso el elegido será WORDFENCE.

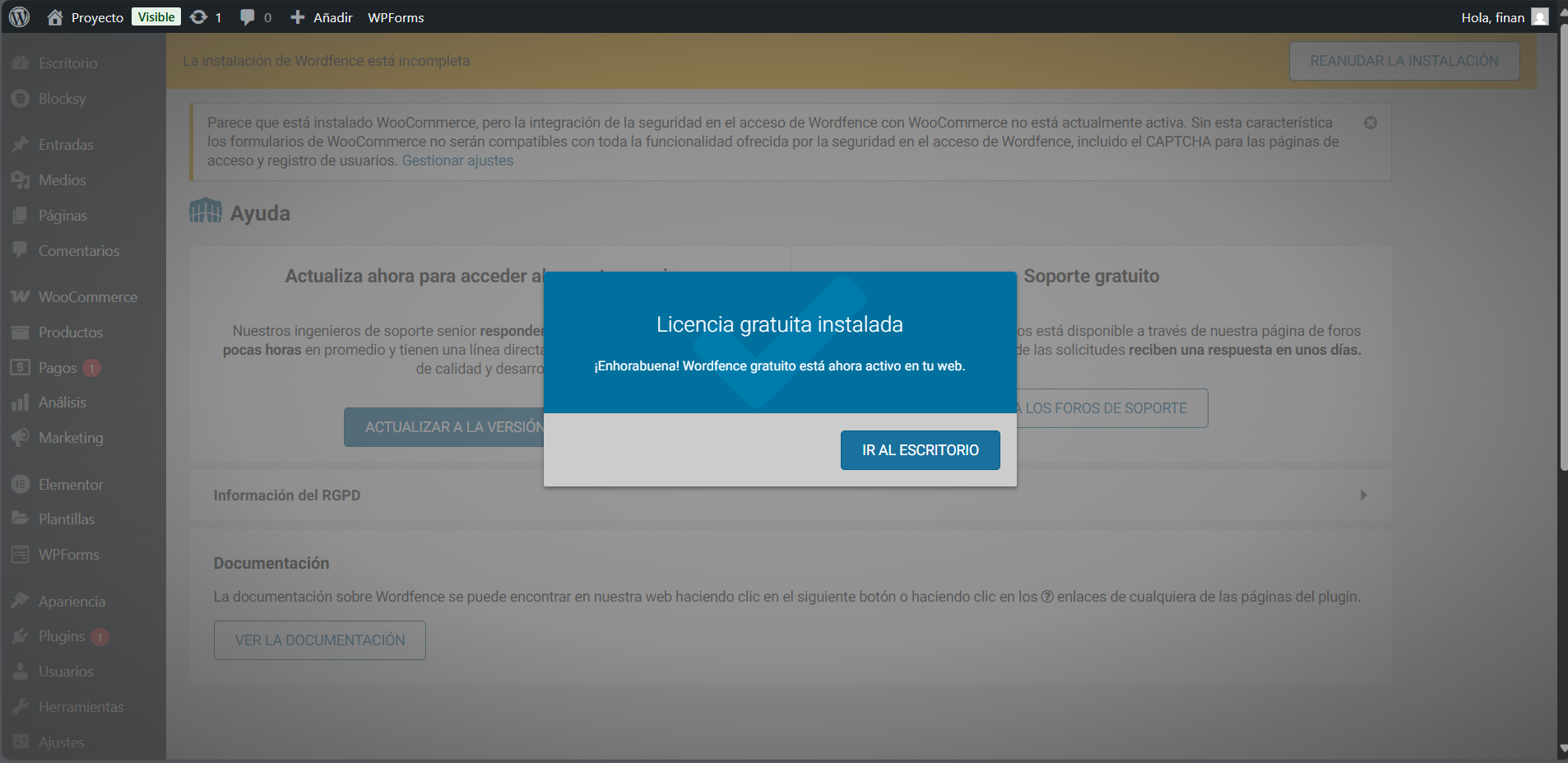
Vemos que no lo tenemos instado, procedemos a instarlo y activarlo como lo podemos ver a continuación.



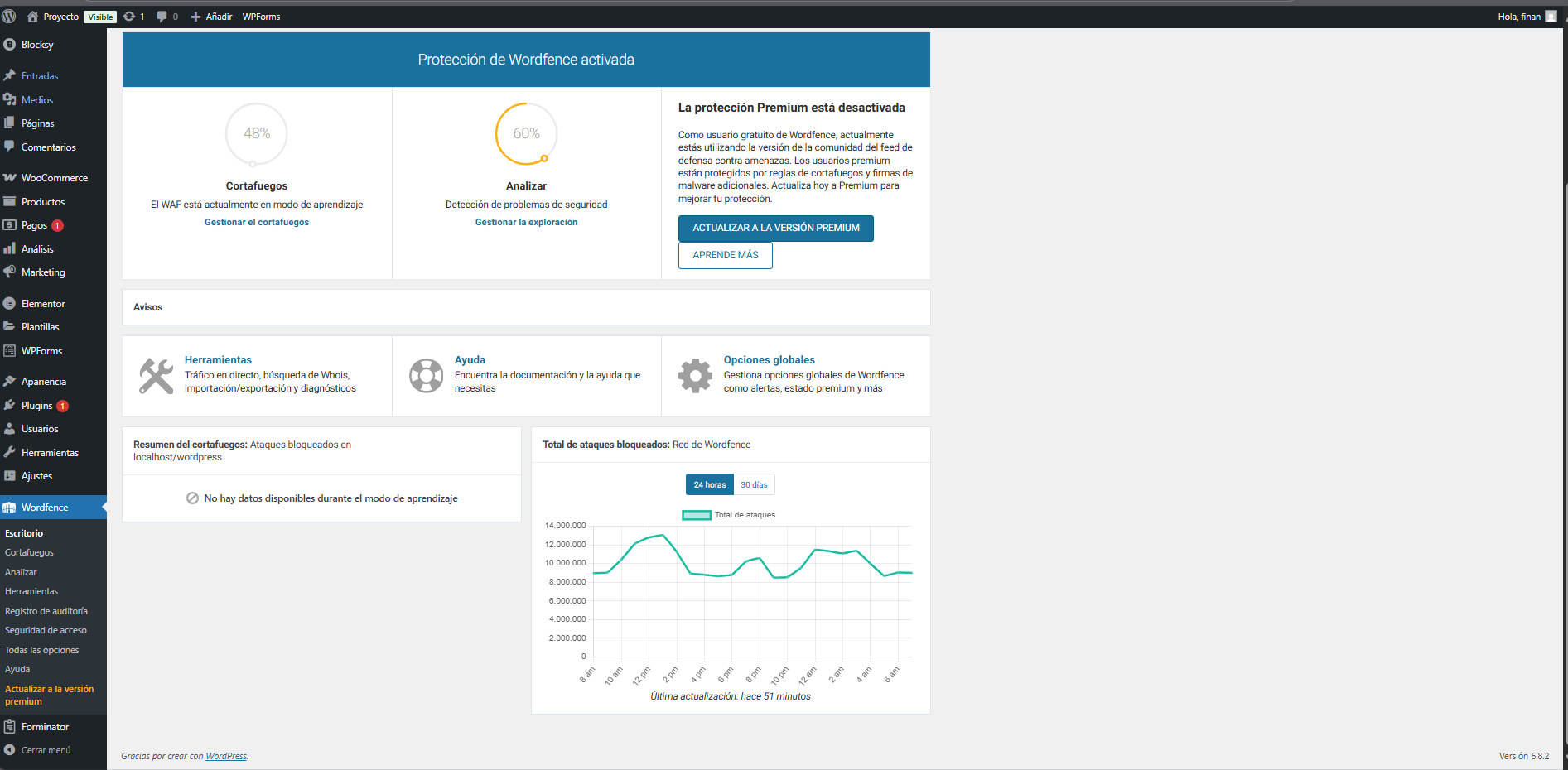
Vemos que no tenemos licencia para acceder, pero nos da una opción free que registramos nuestro correo y listo.

Imagen que contiene Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

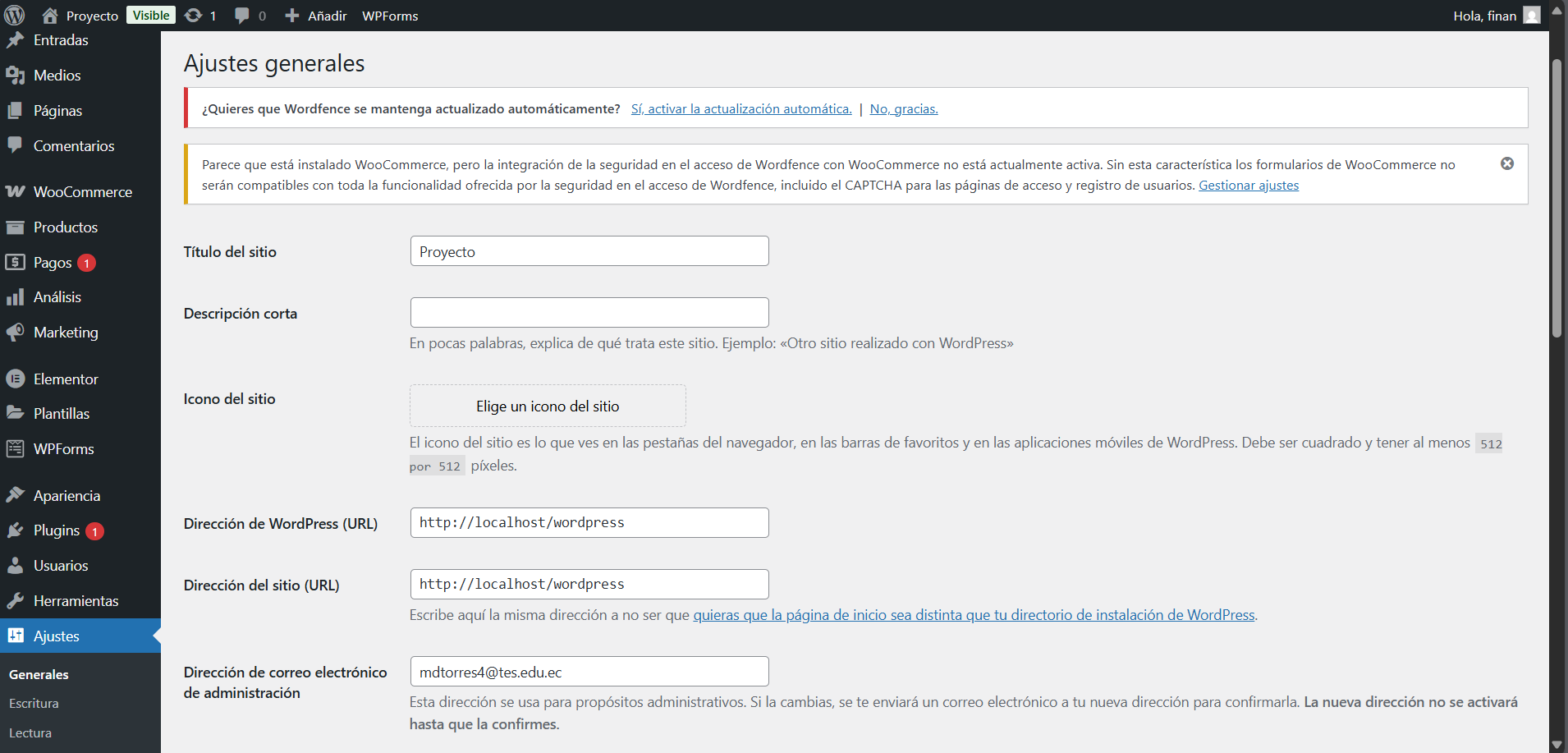


Observamos un análisis que le hace a nuestra página web y como es una página de prueba es obvio que no haya registros, pero con solo descargar nuestra herramienta de seguridad estamos protegidos y aun podemos seguir utilizando más si lo requiere el solicitante de la página o si es propia a su debido criterio.



Ahora vamos a hacer la Configuración de HTTPS.

Nos aseguramos de que nuestra dirección sea https y no como lo vemos en la imagen, continuamos



Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.Utilizaremos un cpanel para nuestra configuración y utilizamos nuestro dominio.

Vemos como nuestro certificado SSL está instalado y listo, ahora podemos ver que nuestro sitio es seguro

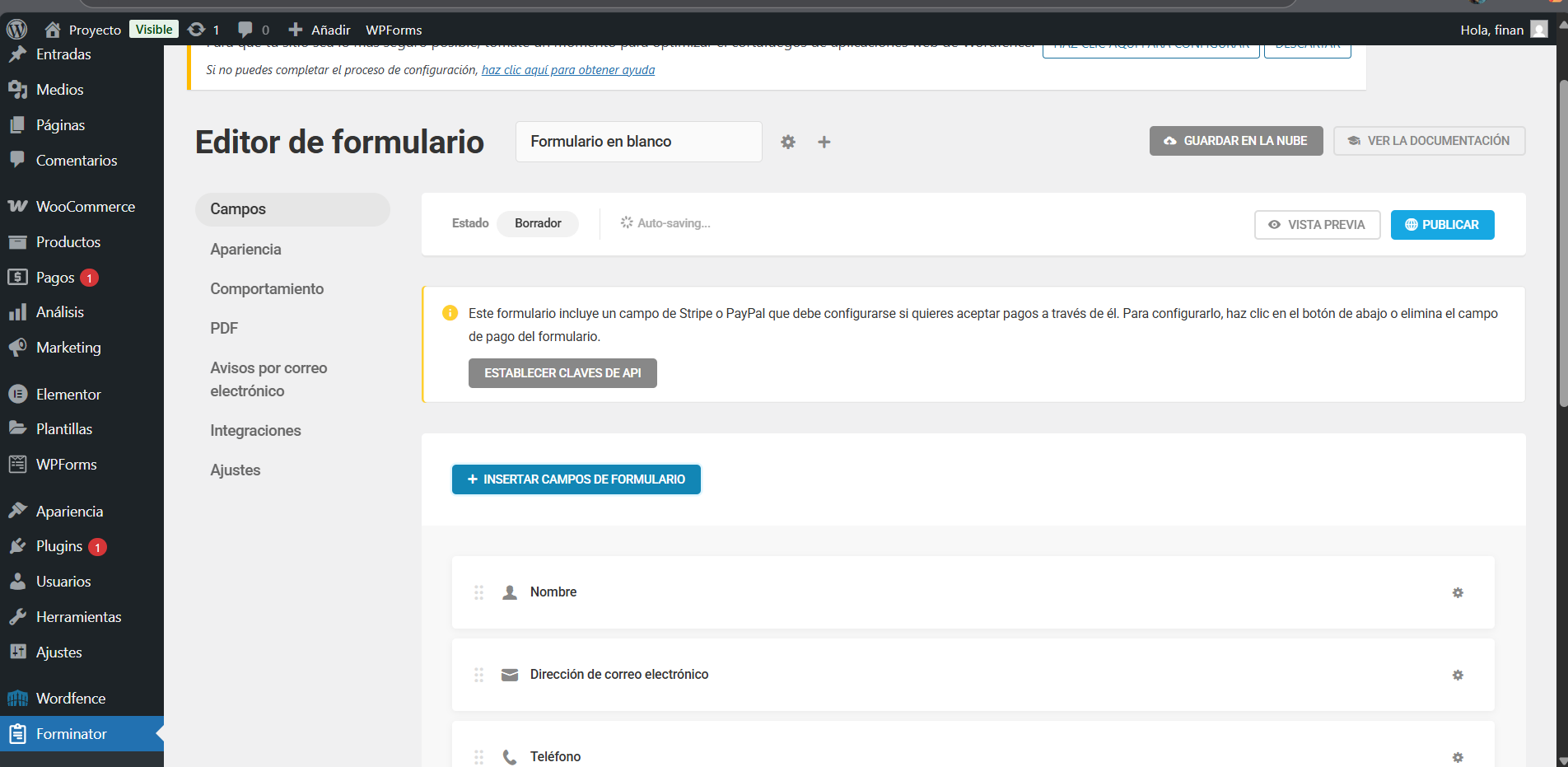
Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

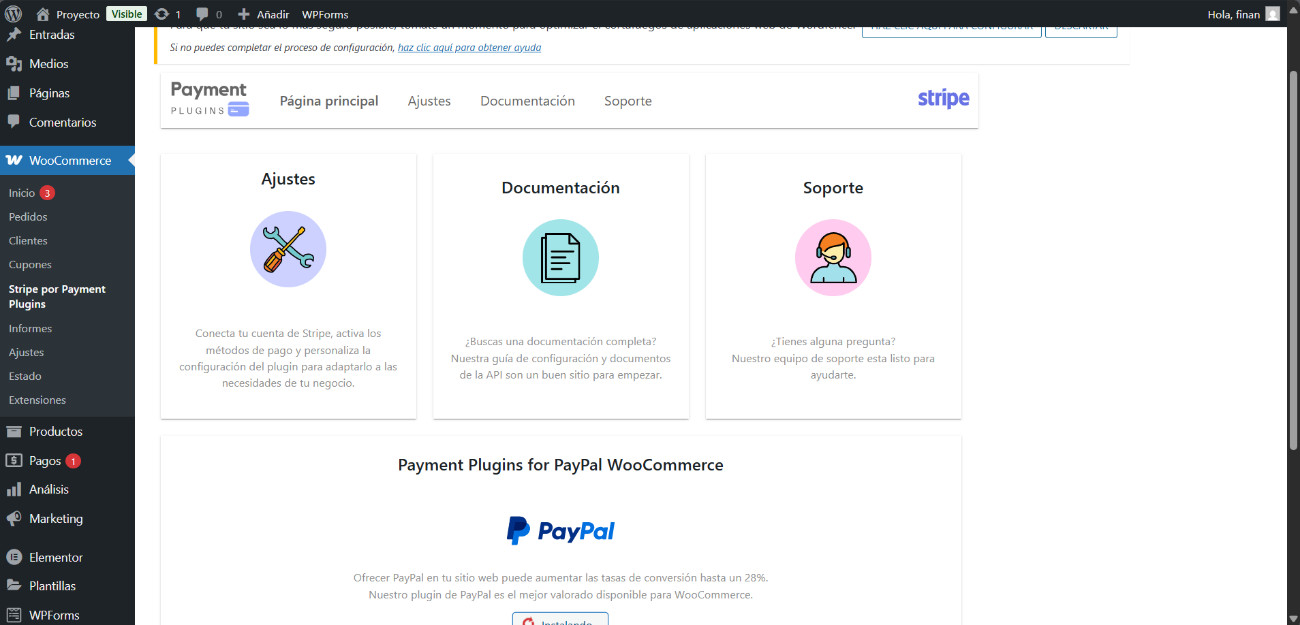
Por último, pero no menos importante para nuestra página web la PASARELA DE PAGOS, utilizamos la herramienta STRIPE.

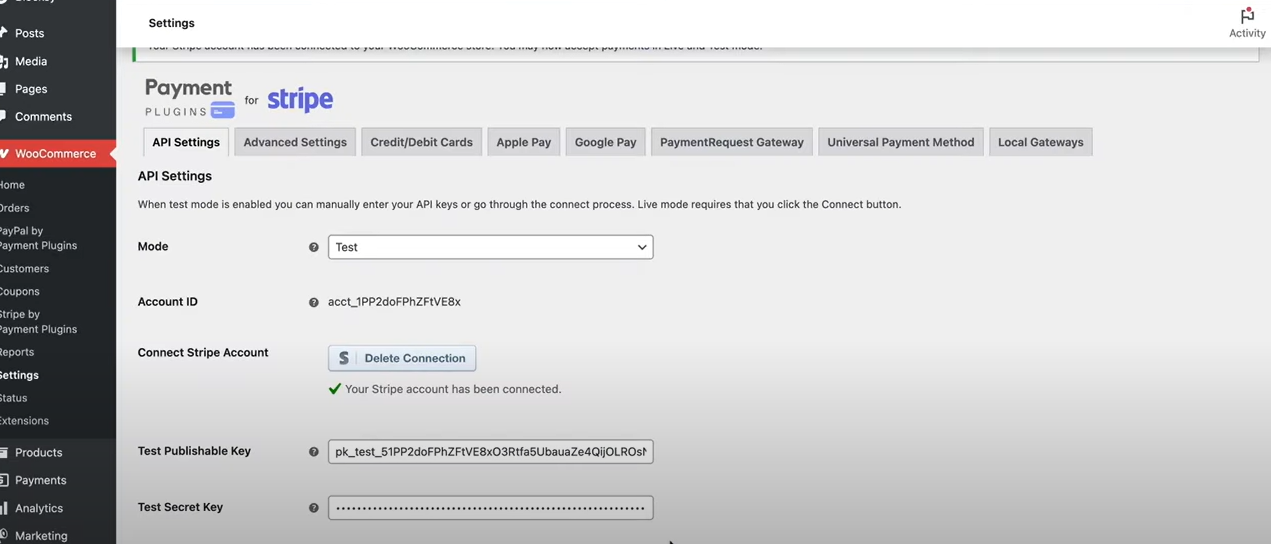
* LLAMADAS API

Como vemos íbamos a realizar nuestra pasarela de pagos, pero nos está requiriendo las llamadas API.



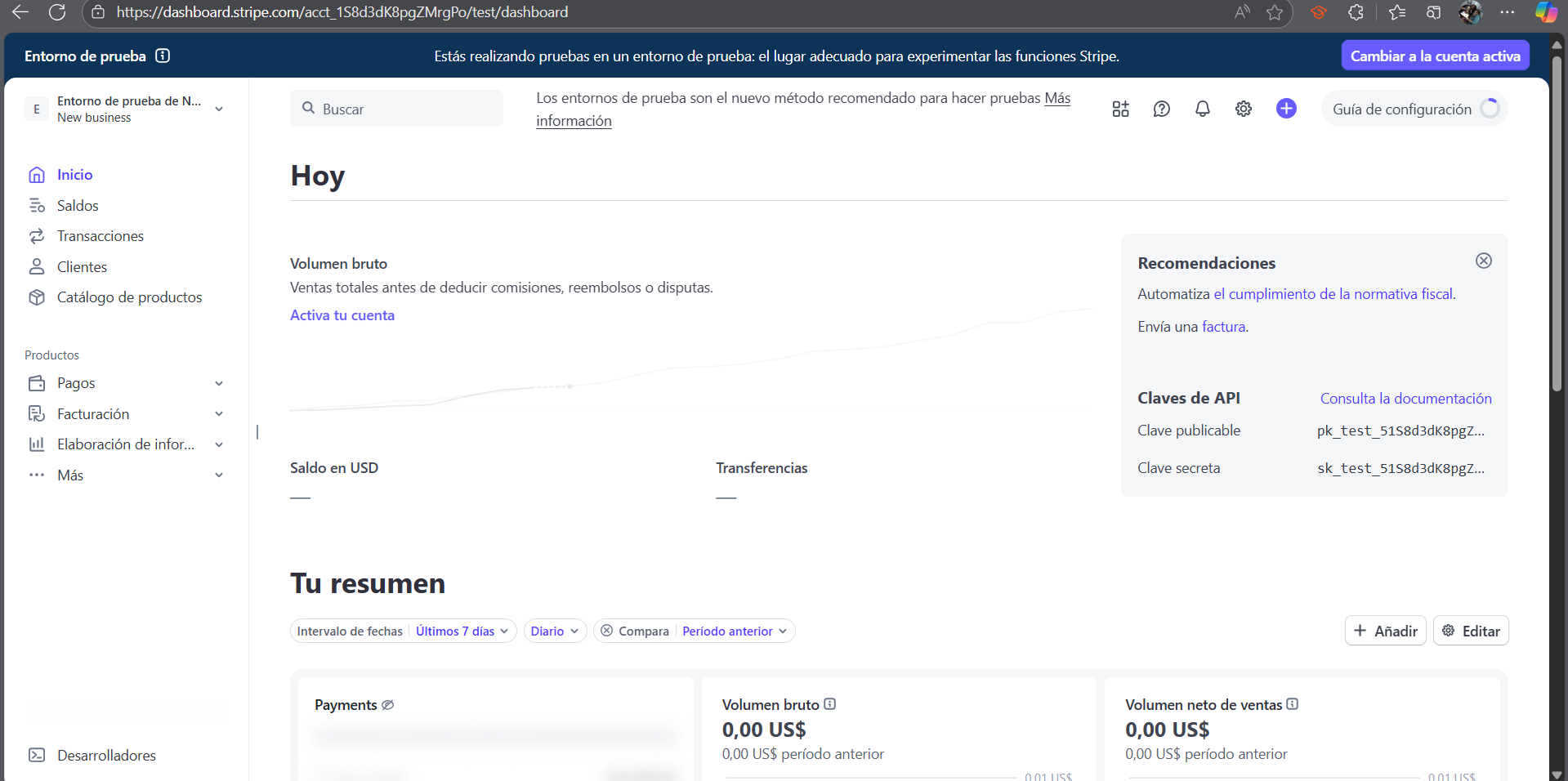
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.Entonces para eso usaremos la herramienta STRIPE, la activamos y dentro de ella nos pide que activemos el plugin de PayPal entonces lo hacemos.

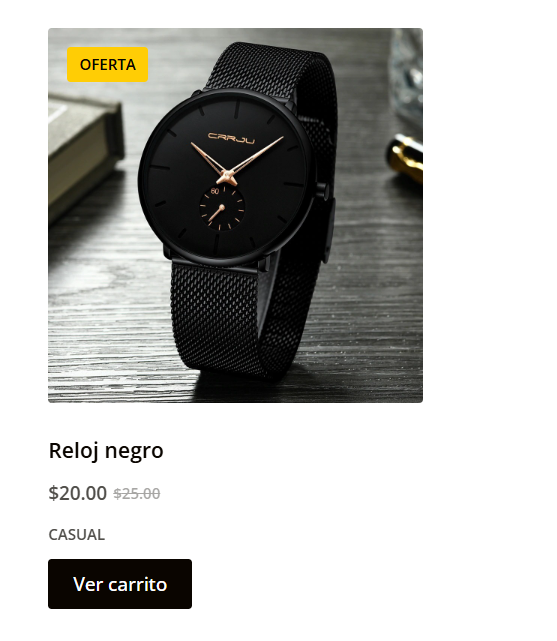
Configuramos 

Y nos damos cuenta de que todo va bien, continuamos con nuestro proyecto

Ahora nos logueamos en la página de stripe como podemos observar estamos dentro del panel de control



Y podemos observar que se ha creado con éxito. Esto permitirá llevar un control con todos los pedidos realizados y con el dinero entrante que va directo a tu Banco Agregado a la cuenta de STRIPE. Ahora nos sale en nuestra página lo siguiente TENEMOS UNA KEY DE PRUEBA Y UNA DE SEGURIDAD.

Nos dirigimos a nuestra pagina web y podemos observar que ahora nos sale esta opción “Ver carrito”:

También podemos observar la pasarela de pagos con toda la información para realizar la compra.

Interfaz de usuario gráfica, Aplicación, Sitio web

El contenido generado por IA puede ser incorrecto.

Proceso de Pago

Se implementó una simulación de pasarela de pagos donde el usuario ingresa: número de tarjeta, fecha de vencimiento y CVC entre otra información. El sistema valida los datos y genera un token de prueba, por ejemplo: tok\_test\_5642. Finalmente muestra la confirmación de pago simulado en la página.



Si el cliente ingresa mal alguna información no se guardará el usuario y debemos realizarlo nuevamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico, Sitio web

El contenido generado por IA puede ser incorrecto.

* + Uso de tokens de pago para no guardar datos sensibles.

**Seguridad en esta simulación**

* Validación de datos del cliente- comprueba tarjeta, fecha y CVC y datos adicionales.
* Uso de tokens: En vez de guardar tu tarjeta, se crea un código de prueba ejemplo: tok\_test\_.
* Nonce de seguridad: WordPress agrega una clave temporal para que nadie pueda falsificar pagos.
* Entorno seguro: como es localhost, no cobra dinero real. En producción se usaría Stripe Test Mode o PayPal Sandbox.

ANALISIS FINAL DE WORDCONFERENCE EN NUESTRA PAGINA:

**Anexo 1: Profundización en Ciberseguridad para un S-SDLC en ToCupboard**

El modelo DevSecOps no solo incorpora la seguridad, sino que la eleva a un nivel de

prioridad al transformar el ciclo de vida del desarrollo de software tradicional en un ciclo

de vida del desarrollo de software seguro. A continuación, se presentan los controles de

ciberseguridad específicos y las acciones fundamentales para cada fase del ciclo de vida

del desarrollo.

**Fase de Planificación y Diseño**

En esta fase inicial, el objetivo primordial es identificar y mitigar los riesgos de seguridad

antes de proceder a la redacción de cualquier línea de código.

**Controles de Ciberseguridad:**

* **Análisis de Amenazas:** Llevar a cabo un análisis estructurado con el fin de identificar las amenazas, vulnerabilidades y posibles ataques al sistema o aplicación. Se pueden emplear metodologías como STRIDE.
* **Análisis de Requisitos de Seguridad:** Establecer y documentar los requisitos de seguridad desde el inicio, tales como la autenticación, autorización, confidencialidad, integridad y disponibilidad.
* **Revisión del Diseño de Arquitectura:** Evaluar la arquitectura de la aplicación y la infraestructura para identificar eventuales puntos débiles o fallas de seguridad.

**Fase de Desarrollo y Codificación**

Aquí se implementan prácticas de codificación segura y se automatizan las revisiones.

Controles de Ciberseguridad

* **Formación en Codificación Segura:** Capacitar a los desarrolladores en las mejores prácticas para evitar vulnerabilidades comunes, como la inyección SQL o el cross-site scripting (XSS).
* **Análisis Estático de la Seguridad de las Aplicaciones (SAST):** Integrar herramientas como SonarQube o Veracode en el entorno de desarrollo (IDE) para escanear el código fuente en busca de vulnerabilidades en tiempo real.
* **Análisis de Composición del Software (SCA):** Utilizar herramientas como OWASP Dependency-Check para escanear las dependencias y librerías de código abierto en busca de vulnerabilidades conocidas (CVEs).

**Fase de Integración y Pruebas**

Esta fase se centra en automatizar las pruebas de seguridad para garantizar que el código integrado no introduzca nuevas vulnerabilidades.

**Controles de Ciberseguridad:**

* **Análisis Dinámico de la Seguridad de las Aplicaciones (DAST):** Ejecutar pruebas automatizadas en la aplicación ya en funcionamiento para simular ataques y descubrir vulnerabilidades. Herramientas como OWASP ZAP son clave.
* **Pruebas de Penetración:** Realizar testing manual o automatizado para encontrar vulnerabilidades que las herramientas automáticas podrían pasar por alto.
* **Escaneo de Contenedores e Imágenes:** Si se usan contenedores (Docker), escanear las imágenes en busca de vulnerabilidades antes de que se desplieguen.

**Fase de Despliegue**

Antes de que el producto sea accesible para los usuarios, se deben realizar verificaciones finales de seguridad en el entorno de producción.

**Controles de Ciberseguridad:**

* **Gestión de Secretos Segura:** Asegurar que las credenciales, claves API y contraseñas no estén codificadas en el código fuente. Se deben usar gestores de secretos como HashiCorp Vault.
* **Análisis de la Configuración de la Infraestructura:** Verificar que la configuración de los servidores, bases de datos y la red cumpla con las políticas de seguridad.
* **Implementación de un Firewall de Aplicaciones Web (WAF):** Desplegar un WAF para proteger la aplicación de ataques comunes como la inyección SQL y XSS.

**Fase de Operaciones y Monitoreo**

La seguridad no termina con el despliegue. Se necesita un monitoreo constante y una respuesta rápida ante incidentes.

**Controles de Ciberseguridad:**

* **Monitoreo y Detección de Amenazas:** Implementar sistemas de gestión de eventos e información de seguridad (SIEM) para recopilar y analizar datos de seguridad en tiempo real y detectar actividades sospechosas.
* **Respuesta a Incidentes:** Tener un plan de respuesta a incidentes bien definido para actuar rápidamente ante una brecha de seguridad.
* **Gestión de Vulnerabilidades Continuas:** Establecer un proceso para escanear y parchear de manera regular las vulnerabilidades que surjan después del despliegue.

Este anexo presenta un alcance detallado de ciberseguridad conforme a la solicitud del experto en el sprint 2, ilustrando de qué manera ToCupboard puede mejorar de manera significativa la seguridad en cada una de las fases del desarrollo. Esto fortalece su propuesta y evidencia una comprensión exhaustiva de las prácticas contemporáneas de seguridad.