JESSIA

Tu tienda en línea segura

Checklist y mini guía de ciberseguridad para WordPress y WooCommerce. Lo esencial, sin tecnicismos.



Jess Calderón
Vender en línea con IA

- Contraseñas
- Servidor y hosting
- Copias de seguridad
- Plugins
- Pagos y bots
- Estafas con IA
- Contracargos
- Checklist de 40 puntos

Guía informativa. No sustituye la asesoría legal ni la de tu banco o pasarela de pago. Más recursos en **jesscalderon.com**.

Tu tienda tiene 7 puertas

Un atacante no necesita entrar por todas. Le basta con una abierta. Y en tu tienda hay pedidos, direcciones y la confianza de tus clientes.



Cómo usar esta guía

1. Lee cada puerta. Son 2 minutos por tema.
2. Marca el checklist de la página 8 con lo que ya tienes.
3. Arregla primero lo que te falte de las puertas 1, 2 y 3.

Mide tu nivel primero

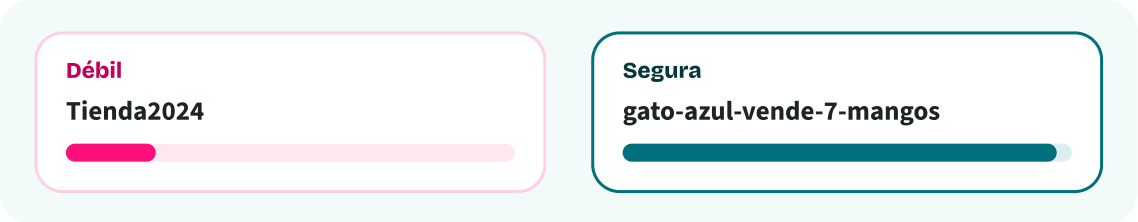
Haz mi **test de ciberseguridad gratis** y vuelve con tu resultado.

Así atacan una tienda WordPress



1 Contraseñas y accesos

La mayoría de los hackeos a WordPress empiezan con una contraseña débil o repetida.



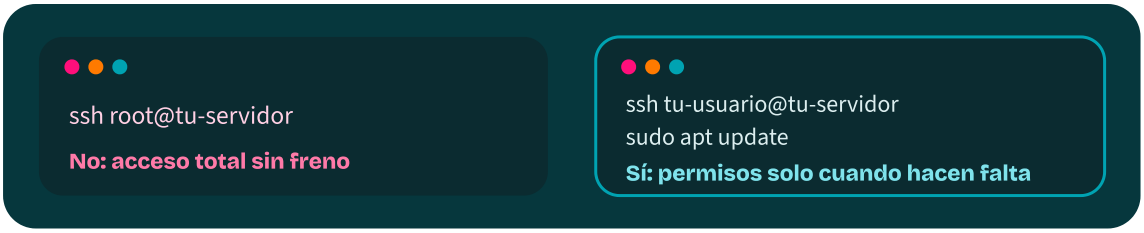
1. **Una contraseña por cuenta.** WordPress, hosting, correo y pasarela, todas distintas.
2. **Usa un gestor** como **Bitwarden** (tiene versión gratis) para no memorizarlas.
3. **Activa la verificación en dos pasos** en wp-admin y en tu correo. Wordfence la trae gratis.
4. **Nunca uses "admin"** como usuario. Crea uno nuevo y borra el viejo.
5. **Da el rol mínimo.** Quien sube productos es "Gestor de tienda", no "Administrador".

Tu correo es la llave maestra

Con él se recuperan todas tus contraseñas. Protégelo primero.

2 Servidor y hosting

Es la casa donde vive tu tienda. Si alguien entra ahí, controla todo lo demás.



1. **Activa la verificación en dos pasos en Hostinger** desde la seguridad de tu cuenta. Es la llave de tu dominio, tu correo y tus copias.
2. **Si tienes VPS o terminal, nunca entres como root.** Crea tu propio usuario con sudo y desactiva el acceso de root por SSH.
3. **Usa llaves SSH** en lugar de contraseña, y SFTP en lugar de FTP.
4. **Mantén el servidor al día:** actualizaciones del sistema y firewall del VPS activo.

3 Copias de seguridad

Si algo sale mal, una copia reciente te regresa a la normalidad en minutos.



1. **Activa las copias del hosting.** En Hostinger están en hPanel, sección Copias de seguridad.
2. **Agrega una copia externa** con **UpdraftPlus** hacia Google Drive o Dropbox.
3. **Mínimo una vez por semana.** Programa la copia automática para no depender de tu memoria.
4. **Haz una copia extra antes de actualizar** plugins, tema o WordPress.

Una copia que no probaste no existe

Cada 3 meses restaura una copia en un subdominio de prueba y revisa que abra.

4 Plugins y actualizaciones

Cada plugin es una puerta más. Menos plugins, menos riesgo.

Antes de instalar, revisa

Que venga de wordpress.org o del sitio oficial. Que se haya actualizado en los últimos 6 meses. Que tenga miles de instalaciones activas y buenas reseñas.

Nunca instales

Plugins o temas "premium gratis" de sitios piratas. Suelen traer código oculto que roba datos o manda spam.

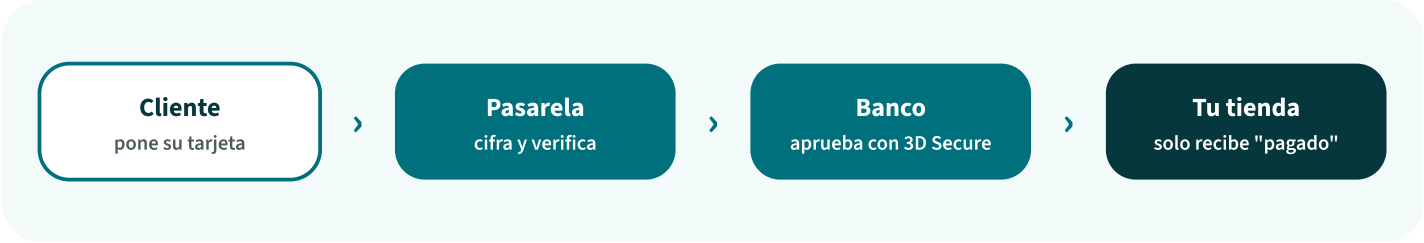
1. **Actualiza cada semana** WordPress, WooCommerce, tema y plugins.
2. **Borra lo que no usas.** Un plugin desactivado sigue siendo un riesgo.
3. **Revisa tu versión de PHP** en el hosting. Usa una versión con soporte vigente.

Instala Wordfence: seguridad en un solo plugin

Es de los plugins de seguridad gratis más usados. Trae firewall, escáner de malware, dos pasos y límite de intentos de acceso. La versión gratis recibe las reglas nuevas 30 días después que la de pago.

5 Pagos y bots

Los datos de la tarjeta nunca deben pasar por tu web. Que los maneje la pasarela.



1. **Usa pasarelas oficiales** para WooCommerce: Stripe, Mercado Pago o PayPal.
2. **Tu sitio siempre con https** y candado, sobre todo en el pago.
3. **Nunca pidas datos de tarjeta** por WhatsApp, correo o formulario.
4. **Revisa pedidos raros** antes de enviar: montos altos, varios intentos fallidos o dirección que no coincide.

Existen 4 tipos de bots

No todos son malos. La clave es dejar pasar a los buenos y frenar a los dañinos.

Buscadores

Googlebot, Bingbot

Te ponen en Google. Déjalos pasar.

Bots de IA

GPTBot, ClaudeBot, CCBot

Leen tu web para la IA. Tú decides en robots.txt.

De servicio

Monitoreo, pasarelas, SEO

Revisan que tu tienda funcione. Son útiles.

Maliciosos

Prueban tarjetas y claves

Copian precios y llenan spam. Bloquéalos.

Firewall contra bots

Cloudflare tiene plan gratis con modo contra bots. El firewall de Wordfence bloquea IPs que atacan muchos sitios WordPress.

Revisión de riesgo por pedido

Stripe incluye Radar, que califica cada pago. Si vendes mucho, una extensión antifraude para WooCommerce frena pedidos sospechosos antes de cobrarlos.

6 Estafas con IA

+33% **El riesgo de fraude en línea va en aumento**

Creció 33% en los primeros cuatro meses de 2026 contra el año anterior. La IA hace los ataques más baratos y más rápidos. Fuente: Signifyd, 2026 State of Fraud Report.

Contra ti y tu equipo

Voz clonada

Llamada con la voz de tu socio o proveedor pidiendo un depósito urgente.

Comprobante falso

Capturas de transferencia hechas con IA para que envíes sin cobrar.

Soporte falso

Correos perfectos "de tu hosting o de WordPress" que piden tu contraseña.

Contra tu tienda

Chatbot engañado

Mensajes hechos para que tu chatbot dé reembolsos, descuentos o datos.

Clientes falsos

Identidades inventadas con IA que compran y luego reclaman al banco.

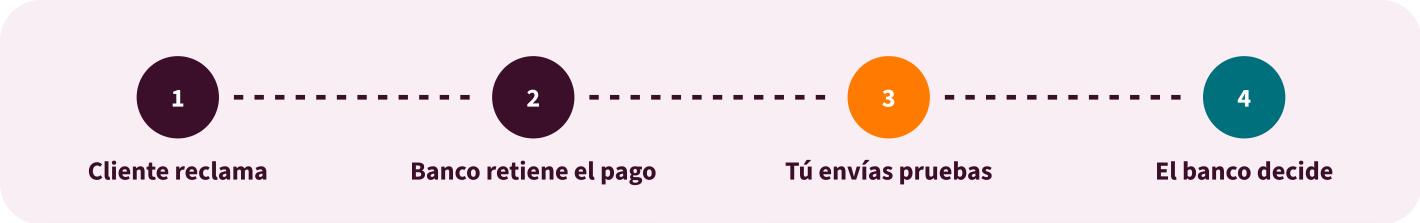
Reseñas falsas

Reseñas negativas muy bien escritas para hundir tus productos.

Riesgo	Qué hacer
Transferencias	Verifica cada pago en tu banco o en el CEP de Banxico. Una captura no es un pago.
Llamadas urgentes	Ten una palabra clave con tu equipo y proveedores. Sin palabra, no hay depósito.
Correos de soporte	Entra siempre desde tu navegador. Ningún soporte real te pide tu contraseña, y "hazlo en 10 minutos" es la señal número uno de estafa.
Chatbot con IA	Que solo responda preguntas frecuentes con tus políticas. Nunca le des permiso de cambiar pedidos ni de reembolsar. Si usas AI Engine, activa la moderación de OpenAI.
Reseñas	En WooCommerce › Ajustes › Productos, permite reseñas solo de propietarios verificados. Usa Akismet contra el spam en formularios.

7 Contracargos

Un contracargo es cuando el cliente pide a su banco que le regrese el dinero de una compra. Si no respondes con pruebas, lo pierdes.



Para prevenirlos

Políticas de envío y devolución visibles. Nombre de tu tienda claro en el estado de cuenta. Guía con rastreo en cada envío.

Para ganarlos

Guarda el pedido, la guía, la confirmación de entrega y los mensajes con el cliente. Responde antes de la fecha límite de tu pasarela.

Reembolsos con candado

1. **Revisa a mano los reembolsos raros:** muchos pedidos chicos, el mismo correo o la misma dirección una y otra vez.
2. **No automatices reembolsos** sin un tope. Los bots buscan justo eso para repetirlo cientos de veces.
3. **Verifica por otro canal** las solicitudes de alto riesgo, como cambio de dirección o reembolso grande. Llama tú al número registrado y haz preguntas fuera de guion.

Preguntas fuera de guion

Un bot responde bien lo que está en el formulario. Pregunta algo que solo sabe el cliente real, como qué producto compró la vez anterior.

Checklist de tu tienda segura

Imprímelo o márcalo en tu celular. Repásalo cada mes.

1 Contraseñas y accesos

- [ ] Contraseña única en WordPress, hosting, correo y pasarela.
- [ ] Uso un gestor de contraseñas.
- [ ] Verificación en dos pasos activa en wp-admin y correo.
- [ ] Ningún usuario se llama "admin".
- [ ] Cada persona tiene el rol mínimo que necesita.
- [ ] Borré usuarios de personas que ya no trabajan conmigo.

2 Servidor y hosting

- [ ] Verificación en dos pasos activa en Hostinger.
- [ ] Nunca entro como root: uso mi usuario con sudo.
- [ ] Acceso por llaves SSH y SFTP, sin FTP.
- [ ] Sistema del VPS actualizado y firewall activo.
- [ ] Tengo a la mano el contacto de soporte de mi hosting.

3 Copias de seguridad

- [ ] Copias automáticas del hosting activas.
- [ ] Copia externa en Google Drive o Dropbox.
- [ ] Copia mínimo una vez por semana.
- [ ] Probé restaurar una copia en los últimos 3 meses.

4 Plugins y actualizaciones

- [ ] Todo actualizado esta semana.
- [ ] Borré temas y plugins que no uso.
- [ ] Cero plugins o temas piratas.
- [ ] Plugin de seguridad con firewall y escaneo.
- [ ] Intentos de acceso limitados.
- [ ] Versión de PHP con soporte vigente.

5 Pagos y bots

- [ ] Sitio completo con https y candado.
- [ ] Pasarela oficial (Stripe, Mercado Pago o PayPal).
- [ ] Nunca pido datos de tarjeta por mensaje.
- [ ] Reviso pedidos sospechosos antes de enviar.
- [ ] Firewall contra bots activo.
- [ ] Revisión de riesgo en cada pago.

6 Estafas con IA

- [ ] Verifico transferencias en el banco, no en capturas.
- [ ] Tengo palabra clave con mi equipo y proveedores.
- [ ] Entro a mis cuentas desde el navegador, no desde correos.
- [ ] Mi chatbot no puede cambiar pedidos ni reembolsar.
- [ ] Reseñas solo de propietarios verificados.
- [ ] Mi equipo sabe que nadie real pide contraseñas.

7 Contracargos

- [ ] Políticas de envío y devolución visibles.
- [ ] Envío con guía y rastreo.
- [ ] Guardo pruebas de cada pedido.
- [ ] Sé dónde responder disputas en mi pasarela.
- [ ] Reviso a mano los reembolsos raros.
- [ ] Verifico por otro canal las solicitudes de alto riesgo.
- [ ] Reembolsos automáticos con tope o desactivados.

¿Cómo saliste?

Cuenta tus casillas marcadas de 40.

34 a 40
Tienda blindada. Repasa cada mes.

20 a 33
Vas bien. Cierra primero las puertas 1, 2 y 3.

0 a 19
Tu tienda está expuesta. Empieza hoy.

Si crees que te hackearon

1. **Cambia contraseñas** desde otro dispositivo: correo, hosting y WordPress.
2. **Avisa a tu hosting.** Pueden revisar y restaurar una copia limpia.
3. **Escanea con Wordfence** y borra lo que no reconozcas.
4. **Revisa tus pasarelas** por pagos o cambios de cuenta que no hiciste.
5. **Avisa a tus clientes** si sus datos pudieron quedar expuestos.

Sigue aprendiendo

Guía completa
Cómo proteger tu tienda en línea, paso a paso.

Test gratis
Mide la seguridad de tu tienda en 2 minutos.

Recursos gratis
Guías y herramientas para vender en línea.



¿Quieres que revise tu tienda contigo?

En una asesoría de ciberseguridad revisamos tu tienda y te digo qué arreglar primero.

Agenda tu asesoría

Jess Calderón · JESSIA · TikTok y YouTube @jessiahacks · jesscalderon.com