Antispam en WordPress sin plugins raros

Honeypot + captcha silencioso + rate limit

Menos fricción, menos spam — setup en 10–15 minutos

Por Fabini | @ilfabini — fabini.one

Made with GAMMA

Checklist rápido: antes de empezar

Antes de implementar cualquier medida antispam, asegúrate de tener todo preparado correctamente. Estas comprobaciones previas garantizan que puedas trabajar con seguridad y revertir cambios si es necesario.

1

Backup reciente verificado

Confirma que tienes una copia de seguridad completa de tu base de datos y archivos. Verifica que puedas restaurarla si algo sale mal. Ideal si es de las últimas 24 horas.

2

Usuario admin con 2FA

Recomendamos encarecidamente que tengas activada la autenticación de dos factores en tu cuenta de administrador. Esto añade una capa extra de seguridad mientras modificas archivos críticos.

3

Acceso a Ajustes y functions.php

Necesitarás acceso al panel de WordPress (Ajustes → Comentarios) y capacidad para editar functions.php vía tema hijo o plugin Code Snippets. Si no tienes tema hijo, crea uno primero.

Con estas tres comprobaciones completadas, estás listo para implementar las medidas antispam de forma segura. El proceso completo no debería llevarte más de 15 minutos si sigues los pasos ordenadamente.

Made with GAMMA

Ajustes nativos de WordPress

Configuración básica en 1 minuto

WordPress incluye herramientas antispam integradas que muchos administradores pasan por alto. Estos ajustes nativos son tu primera línea de defensa y no requieren código adicional.

Dirígete a **Ajustes → Comentarios** en tu panel de WordPress y aplica las siguientes configuraciones:

Aprobación manual inicial

Activa la opción "Un comentario debe ser aprobado manualmente" solo para el primer comentario de cada usuario. Esto filtra spambots que no vuelven.

Cierre automático temporal

Configura el cierre automático de comentarios en entradas con más de 14 días. El spam suele atacar contenido antiguo que ya no monitoreas activamente.

Lista de palabras prohibidas

Añade 5–10 términos específicos de spam que hayas detectado en tu sitio: marcas de medicamentos, casino, préstamos, etc. Personaliza según tu experiencia.

Correo obligatorio, web opcional

Exige dirección de correo electrónico válida pero no hagas obligatorio el campo "sitio web". Menos campos = menos spam de enlaces.

Estos cuatro ajustes nativos ya reducirán significativamente el spam sin afectar la experiencia de usuarios legítimos. Son reversibles en cualquier momento desde el mismo panel.

Made with GAMMA

Eliminar el campo URL de comentarios

El campo "sitio web" en los formularios de comentarios es un imán para spammers que buscan conseguir backlinks gratuitos. Al eliminarlo, reduces drásticamente los comentarios cuyo único objetivo es dejar un enlace.

La mayoría de comentaristas legítimos no necesitan compartir su URL. Si alguien realmente quiere promocionar su sitio, puede incluirlo en el contenido del comentario (donde puedes moderarlo). Esta simple modificación puede reducir el spam hasta un 40% según nuestra experiencia.

Código para functions.php (tema hijo)

```
/* Elimina el campo URL del formulario de comentarios */
add_filter('comment_form_default_fields', function($fields){
    if (isset($fields['url'])) {
        unset($fields['url']);
    }
    return $fields;
});
```

Añade este código al archivo **functions.php** de tu tema hijo, o mejor aún, utiliza un plugin como **Code Snippets** para mantener las modificaciones separadas del tema. Si cambias de tema en el futuro, tus personalizaciones permanecerán intactas.

Nota importante: Después de añadir este código, limpia la caché de tu sitio y comprueba el formulario de comentarios en modo incógnito para verificar que el campo ha desaparecido correctamente. Algunos temas pueden tener estilos CSS que lo oculten visualmente pero no lo eliminen del HTML.

Menos enlaces salientes en tu sitio también mejora ligeramente tu SEO, ya que Google valora que no enlaces indiscriminadamente a sitios externos de baja calidad.

Made with GAMMA

Honeypot invisible: trampa para bots

Un honeypot (campo trampa) es una técnica elegante que añade un campo invisible al formulario. Los humanos no lo ven ni lo rellenan, pero los bots automatizados sí completan todos los campos que encuentran. Si ese campo llega relleno al servidor, sabemos con certeza que es spam.

Esta técnica es extremadamente efectiva contra spambots básicos e intermedios, bloqueando aproximadamente el 60–70% del spam automatizado sin molestar a usuarios reales. No requiere JavaScript, funciona en cualquier navegador y es compatible con lectores de pantalla si se implementa correctamente.

Paso A: Añadir el campo trampa al formulario

```
/* Añade input honeypot invisible al formulario de comentarios */
add_action('comment_form_after_fields', function(){
    echo '<p style="display:none !important;" aria-hidden="true">
        <label for="hp_field">Deja este campo vacío</label>
        <input type="text" name="hp_field" id="hp_field" value="" />
    </p>';
});
```

Este código inserta un campo de texto completamente oculto mediante CSS. El atributo **aria-hidden="true"** garantiza que los lectores de pantalla lo ignoren, manteniendo la accesibilidad para usuarios con discapacidad visual.

Paso B: Validar en el servidor

```
/* Si el honeypot viene relleno → bloquear el comentario */
add_filter('preprocess_comment', function($commentdata){
    if (!empty($_POST['hp_field'])) {
        wp_die(__('Spam detectado. Tu comentario no ha sido enviado.'));
    }
    return $commentdata;
});
```

Cuando WordPress procesa un comentario, este filtro comprueba si el campo honeypot contiene algún valor. Si es así, detiene el proceso inmediatamente mostrando un mensaje de error. Los bots no ven este mensaje, pero tú sí lo verás en tus logs si quieres monitorizar cuánto spam estás bloqueando.

Consejo de seguridad

Cambia el nombre del campo (**hp_field**) periódicamente cada 3–6 meses. Utiliza nombres poco obvios como **website_url_check** o **validation_token**. Algunos bots sofisticados identifican honeypots con nombres genéricos.

Combinación perfecta

El honeypot funciona excepcionalmente bien combinado con las demás técnicas de este documento. No pongas todos tus huevos en una sola cesta: la estrategia multicapa es la más efectiva.

Made with GAMMA

reCAPTCHA v3 y Cloudflare Turnstile

Captcha silencioso sin puzzles frustrantes

Los captchas tradicionales (identificar semáforos, escribir texto distorsionado) frustran a los usuarios. Las versiones modernas como **reCAPTCHA v3** y **Cloudflare Turnstile** trabajan en segundo plano, analizando el comportamiento del usuario sin interrumpir la experiencia.

reCAPTCHA v3 asigna una puntuación de 0.0 a 1.0 según la probabilidad de que sea humano. Tú decides el umbral: 0.5 es equilibrado, 0.3 más permisivo, 0.7 más estricto. Turnstile de Cloudflare ofrece funcionalidad similar con mejor privacidad y sin depender de Google.

Obtén tus claves

Regístrate en Google reCAPTCHA o Cloudflare y genera tu **Site Key** y **Secret Key**. Guárdalas en un lugar seguro.

Integra con tu plugin

WPForms, Contact Form 7 y Gravity Forms tienen campos nativos para reCAPTCHA/Turnstile. Introduce tus claves en la configuración del plugin.

Ajusta el umbral

Empieza con score 0.5 y monitoriza falsos positivos durante una semana. Ajusta si es necesario: más alto = más estricto.

Comparación: reCAPTCHA v3 vs Turnstile

Característica	reCAPTCHA v3	Cloudflare Turnstile
Privacidad	Google analiza datos del usuario	Mayor privacidad, sin tracking invasivo
Configuración	Sencilla, amplia documentación	Muy sencilla, integración Cloudflare
Compatibilidad	Soportado por casi todos los plugins	Creciendo rápidamente, menos plugins
Coste	Gratuito hasta 1M peticiones/mes	Gratuito sin límites claros
Experiencia usuario	Invisible, sin interacción	Invisible, sin interacción

Ambas soluciones son excelentes. Si ya usas Cloudflare para tu sitio, Turnstile es la opción natural. Si prefieres el ecosistema de Google o necesitas compatibilidad universal, reCAPTCHA v3 es tu mejor apuesta.

Campos de configuración: Sustituye `[[SITE_KEY]]` y `[[SECRET_KEY]]` con tus claves reales en la configuración de tu plugin. Nunca compartas la Secret Key públicamente ni la incluyas en código JavaScript del frontend.

Made with GAMMA

Rate limiting: control de frecuencia

El rate limiting (limitación de tasa) restringe cuántas peticiones puede hacer una IP en un intervalo de tiempo. Si alguien intenta enviar 50 comentarios en un minuto, claramente es un bot. Esta técnica complementa perfectamente honeypots y captchas, actuando como última línea de defensa.

Implementar rate limiting efectivo requiere herramientas a nivel de servidor o WAF (Web Application Firewall). Las soluciones en WordPress (vía PHP) son menos eficientes porque el código PHP ya se ha ejecutado cuando detectas el abuso. Lo ideal es bloquearlo antes de que llegue a WordPress.

Opción A: Cloudflare (recomendado)

Si tu sitio usa Cloudflare (incluso en plan gratuito), puedes crear reglas de rate limiting personalizadas desde el panel. Dirígete a **Security → WAF → Rate limiting rules** y configura:

01

Define la ruta objetivo

Aplica la regla cuando la URI contiene **/wp-comments-post.php** o **/wp-login.php** (para proteger también el login de ataques de fuerza bruta).

02

Establece el límite

Configura un máximo de 5–10 peticiones por minuto desde la misma IP. Los usuarios humanos raramente envían más de 2–3 comentarios/minuto.

03

Elige la acción

Selecciona "Block" para bloquear directamente, o "Challenge" para mostrar un captcha interactivo. "Block" es más agresivo pero efectivo.

04

Monitoriza y ajusta

Revisa el dashboard durante 48 horas. Si ves IPs legítimas bloqueadas (falsos positivos), aumenta el límite a 15–20 peticiones/minuto.

Opción B: Regla .htaccess (limitada)

Si no usas Cloudflare ni tienes acceso a configuración de servidor avanzada, puedes añadir esta regla básica a tu archivo **.htaccess** en la raíz de WordPress:

```
# Protección básica de wp-comments-post.php
<Files "wp-comments-post.php">
    Require all granted
    # Nota: el rate limiting real requiere módulos
    # como mod_evasive o mod_qos en Apache
    # Esta regla solo documenta el archivo a proteger
</Files>
```

Limitación de .htaccess: Apache no tiene rate limiting nativo en .htaccess básico. Necesitas módulos como **mod_evasive**, **mod_qos** o **mod_security** instalados en el servidor. Contacta con tu proveedor de hosting para confirmar disponibilidad. Para rate limiting efectivo sin acceso al servidor, Cloudflare es tu mejor opción.

El rate limiting es especialmente efectivo contra ataques distribuidos (botnets) que intentan saturar tu formulario desde múltiples IPs. Combinado con honeypot y captcha silencioso, crea una defensa multicapa prácticamente impenetrable para spam común.

Made with GAMMA

Protección de formularios de contacto

Los formularios de contacto son tan vulnerables al spam como los comentarios, pero muchos administradores olvidan protegerlos. Aplica las mismas técnicas que hemos visto: honeypot, reCAPTCHA/Turnstile y rate limiting.

La mayoría de plugins populares de formularios —Contact Form 7, WPForms, Gravity Forms, Formidable— incluyen opciones integradas para estas protecciones. No necesitas código personalizado, simplemente activar las funciones desde sus respectivos paneles de configuración.

Contact Form 7

Instala el plugin **Flamingo** para almacenar envíos y el addon **reCAPTCHA** oficial. Configura tus claves en **Integración → reCAPTCHA** y añade la etiqueta [recaptcha] a tus formularios.

WPForms

Ve a **WPForms → Settings → CAPTCHA**. Selecciona reCAPTCHA v3 o hCaptcha, introduce tus claves y activa en los formularios que desees. También tiene honeypot integrado en la sección Anti-spam.

Gravity Forms

Accede a **Forms → Settings → reCAPTCHA**. Configura tus claves y luego, en cada formulario individual, añade el campo reCAPTCHA desde el editor visual. Muy sencillo y sin código.

Buenas prácticas adicionales

- **Nunca muestres direcciones de email en texto plano** en tu sitio. Los scrapers las recopilan para spam. Usa siempre formularios de contacto.
- **Evita enlaces "mailto:"** en el HTML. Si necesitas mostrar un email, usa JavaScript para ofuscarlo o mejor aún, redirige a un formulario.
- **Valida campos en servidor y cliente.** La validación JavaScript mejora UX, pero la validación PHP en servidor es la que realmente importa para seguridad.
- **Limita el tamaño de archivos adjuntos** a 2–5 MB. Algunos bots intentan saturar tu servidor subiendo archivos enormes repetidamente.
- **Desactiva formularios en páginas antiguas** que ya no monitoreas. Si tienes una landing page de 2019 que ya no usas, desactiva su formulario.

Los formularios de contacto protegidos no solo evitan spam, también previenen ataques más serios como inyección de código o intentos de phishing que suplantan tu dominio. Dedica 5 minutos a configurarlos correctamente y olvídate del problema durante años.

Made with GAMMA

Verificación, pruebas y seguimiento

Implementar medidas antispam sin verificar su efectividad es como instalar una alarma sin comprobar que funciona. Dedica tiempo a probar cada capa de protección y establece un sistema de seguimiento para medir resultados a lo largo del tiempo.

Checklist de verificación inmediata

- **Prueba de usuario real**

  Abre una ventana de incógnito (sin sesión de WordPress) y envía un comentario o formulario legítimo. Debe pasar sin problemas. Si hay captcha, no debería mostrarse o debería ser invisible.

- **Verifica el honeypot**

  Inspecciona el HTML del formulario (clic derecho → Inspeccionar elemento). Confirma que el campo trampa está presente pero completamente oculto con **display:none** y **aria-hidden**.

- **Simula comportamiento de bot**

  Usando las herramientas de desarrollador del navegador, quita el **display:none** del honeypot, rellénalo con texto y envía. Debería bloquearse con mensaje "Spam detectado".

- **Comprueba moderación**

  Ve a **Comentarios** en tu panel de WordPress. Los comentarios de nuevos usuarios deberían aparecer en "Pendientes" si activaste aprobación manual del primero.

- **Revisa logs de Cloudflare**

  Si configuraste rate limiting en Cloudflare, ve a **Security → Events** para ver peticiones bloqueadas. Deberías ver actividad de bots bloqueados en las primeras 24–48 horas.

Tabla de seguimiento semanal (primeras 4 semanas)

Semana	Spam bloqueado	Falsos positivos	Ajuste realizado	Notas
1	~87 intentos	2 legítimos	Score captcha 0.5→0.4	Efectivo
2	~63 intentos	0	Ninguno	Estable
3	~45 intentos	1 legítimo	Revisión manual OK	Mejora
4	~30 intentos	0	Ninguno	Óptimo

Es completamente normal ver una reducción gradual del spam durante las primeras semanas. Los bots eventualmente "aprenden" que tu sitio está protegido y dejan de intentarlo con tanta frecuencia. Si después de 30 días sigues recibiendo spam significativo, considera añadir capas adicionales como Akismet o servicios premium.

Monitorización a largo plazo

Revisa tus comentarios pendientes cada 48–72 horas durante el primer mes para detectar falsos positivos. Un comentario legítimo bloqueado por error daña la confianza del usuario. Después del periodo inicial, una revisión semanal es suficiente.

Documenta cualquier patrón de spam que notes (idiomas específicos, palabras recurrentes, rangos de IP) para afinar tu lista de palabras prohibidas en **Ajustes → Comentarios**. El antispam es un proceso iterativo, no una configuración única.

Made with GAMMA

Errores comunes y soluciones rápidas

Incluso siguiendo esta guía al pie de la letra, pueden surgir pequeños problemas de configuración. Aquí documentamos los errores más frecuentes que vemos en implementaciones antispam y cómo solucionarlos en minutos.

Honeypot visible por CSS roto

Síntoma: El campo trampa aparece visible en el formulario, confundiendo a usuarios reales.

Causa: Tu tema tiene estilos CSS que anulan el **display:none** del honeypot, o el código no incluyó **!important**.

Solución: Añade **!important** al estilo inline: `style="display:none !important;"` y confirma que el atributo **aria-hidden="true"** está presente. Limpia caché del sitio y navegador.

Turnstile o reCAPTCHA no carga

Síntoma: El widget del captcha no aparece en el formulario, o muestra error de carga.

Causa: El script de captcha está siendo bloqueado por plugins de caché o tu CDN no sirve correctamente archivos JavaScript externos.

Solución: Excluye las páginas con formularios del sistema de caché (en WP Rocket: **Excluded Pages**). Si usas Cloudflare, desactiva Rocket Loader en esas URLs específicas. Verifica en consola del navegador (F12) si hay errores de carga del script.

Rate limiting bloquea demasiado

Síntoma: Usuarios legítimos reportan que no pueden comentar o enviar formularios, ven mensajes de error 429.

Causa: El umbral de rate limiting está demasiado bajo (ej: 3 peticiones/minuto) o tu IP compartida afecta a múltiples usuarios.

Solución: Aumenta el límite a 15–20 peticiones/minuto en Cloudflare. Si usas hosting compartido, considera activar rate limiting solo en **wp-login.php** y dejarlo más permisivo en **wp-comments-post.php**. Revisa el log de eventos en Cloudflare para identificar IPs bloqueadas legítimas y añádelas a una whitelist.

Comentarios legítimos en spam

Síntoma: Comentarios claramente humanos van a la carpeta de spam o quedan pendientes indefinidamente.

Causa: El score de reCAPTCHA v3 está demasiado alto (ej: 0.8) o tu lista de palabras prohibidas es excesivamente agresiva.

Solución: Reduce el score a 0.4–0.5 y revisa tu lista de palabras prohibidas en **Ajustes → Comentarios**. Elimina términos demasiado genéricos. Considera whitelist de IPs para usuarios conocidos frecuentes. Si usas Akismet junto a estas medidas, puede haber conflicto; desactiva uno temporalmente para identificar el culpable.

Hoja de seguimiento: plantilla para 30 días

Copia esta tabla en una hoja de cálculo y rellena diariamente durante el primer mes para detectar patrones:

Día	Spam bloqueado	Falsos positivos	Ajuste realizado	Notas adicionales
1	[[rellenar]]	[[rellenar]]	[[rellenar]]	[[rellenar]]
2–30	[[continuar]]	[[continuar]]	[[continuar]]	[[continuar]]

Conclusión: bandeja limpia, usuarios felices

Implementar honeypot + captcha silencioso + rate limiting te da una protección robusta sin sacrificar experiencia de usuario. La configuración inicial toma 10–15 minutos, pero te ahorrará horas cada semana limpiando spam manualmente.

Recuerda: **el antispam efectivo es multicapa**. Ninguna técnica individual bloquea el 100% del spam, pero combinadas crean una barrera que solo el spam más sofisticado (y raro) puede atravesar. Y ese porcentaje residual puedes moderarlo manualmente sin problema.

> **Más guías prácticas en fabini.one**
>
> Si esta guía te ha ayudado, etiqueta **@fabinidc** en redes sociales. Tu feedback ayuda a crear mejores recursos para la comunidad.

Nota legal: Esta guía se proporciona con fines educativos. Implementa bajo tu responsabilidad y realiza siempre backups antes de modificar archivos de tu sitio. El autor no se responsabiliza de problemas técnicos derivados de configuraciones incorrectas.

Made with GAMMA