Guía de Seguridad

Fecha de publicación: 21/01/2021

Tema: Guía de Seguridad contra SPAM *Bots* en WordPress

Objetivo: Proveer instrucciones sobre cómo evitar y hacer frente a ataques de SPAM contra WordPress para tres escenarios posibles: resultados de búsqueda negativos en Google, comentarios en publicaciones y registro masivo de usuarios en el sitio WordPress; para reducir el potencial riesgo de dichos ataques y evitar que la reputación del sitio sea dañada por atacantes mal intencionados.

Escenario 1 - Cómo configurar sitio WordPress para evitar SPAM *bots* en buscadores

A la hora de llevar a cabo la configuración, se debe tener en cuenta dos posibles alternativas de prevención:

- Uso del meta *tag* “robots”.
- Configuración del archivo robots.txt

¿Dónde configurarlo?

La primera alternativa es la utilización del meta *tag* “robots” con el contenido "no index" para evitar la indexación del contenido de la página dada por parte de los buscadores. Puede agregarse la siguiente línea al código HTML del sitio web:

```
<meta name="robots" content="noindex">
```

La segunda alternativa es la utilización del archivo **“robots.txt”** definiendo una directiva para prevenir los ataques mencionados. Pueden agregarse las siguientes líneas al archivo:

```
User-agent: *

Disallow: /?s=
```

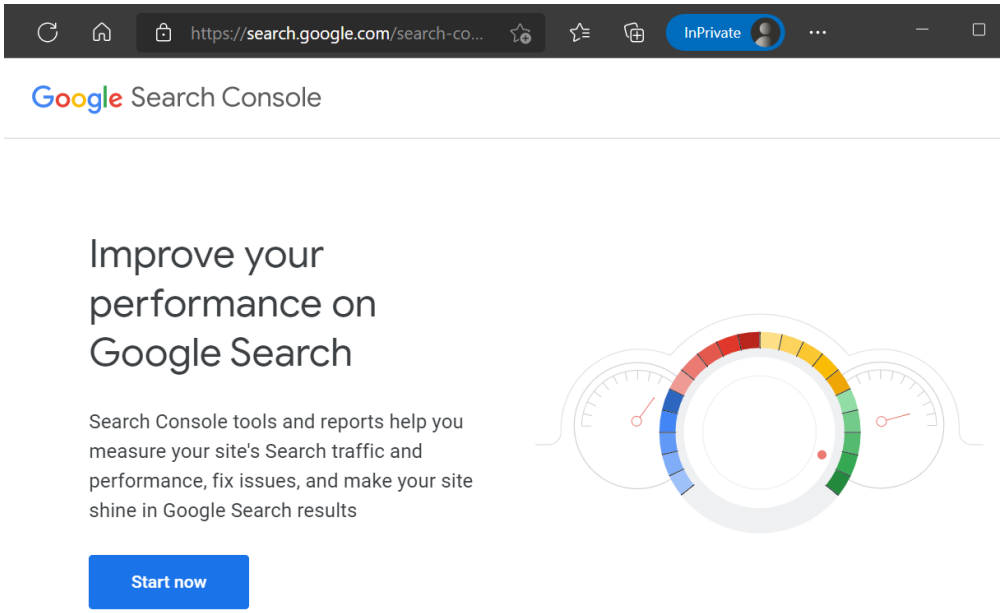
La misma indica que cualquier bots o todos los bots (**"*"**) no tienen permitido indexar o hacer scrapping de la ruta "**/?s="** , dicha ruta representa el buscador interno del sitio WordPress.

Para más información sobre ambas alternativas remitirse al siguiente enlace proveído por Google.

Adicionalmente, es recomendable remover páginas e índices no deseados de la búsqueda de Google mediante la herramienta Google Search Console. Para ello se debe enviar y verificar su sitio en la consola de búsqueda de Google.

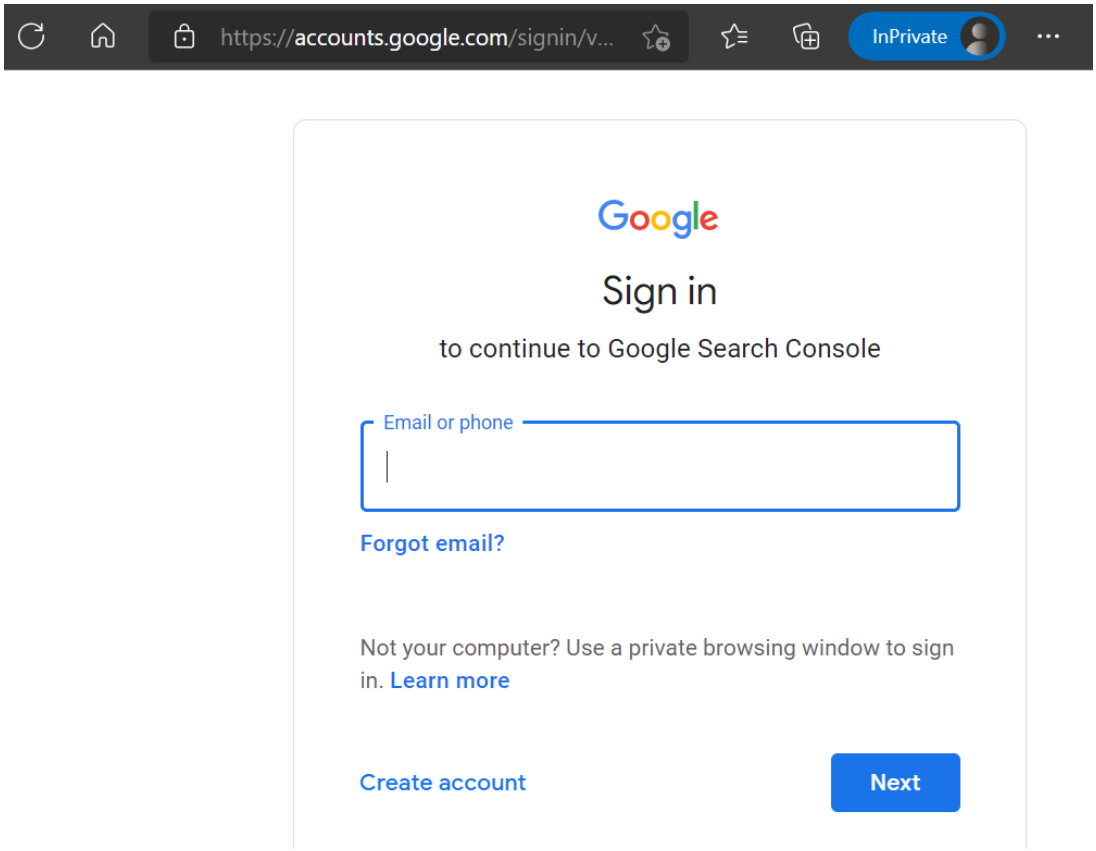
Para enviar un sitio a Google Search Console se deben seguir los siguientes pasos:

1. Visitar la página de la consola de Google Search en el siguiente enlace.

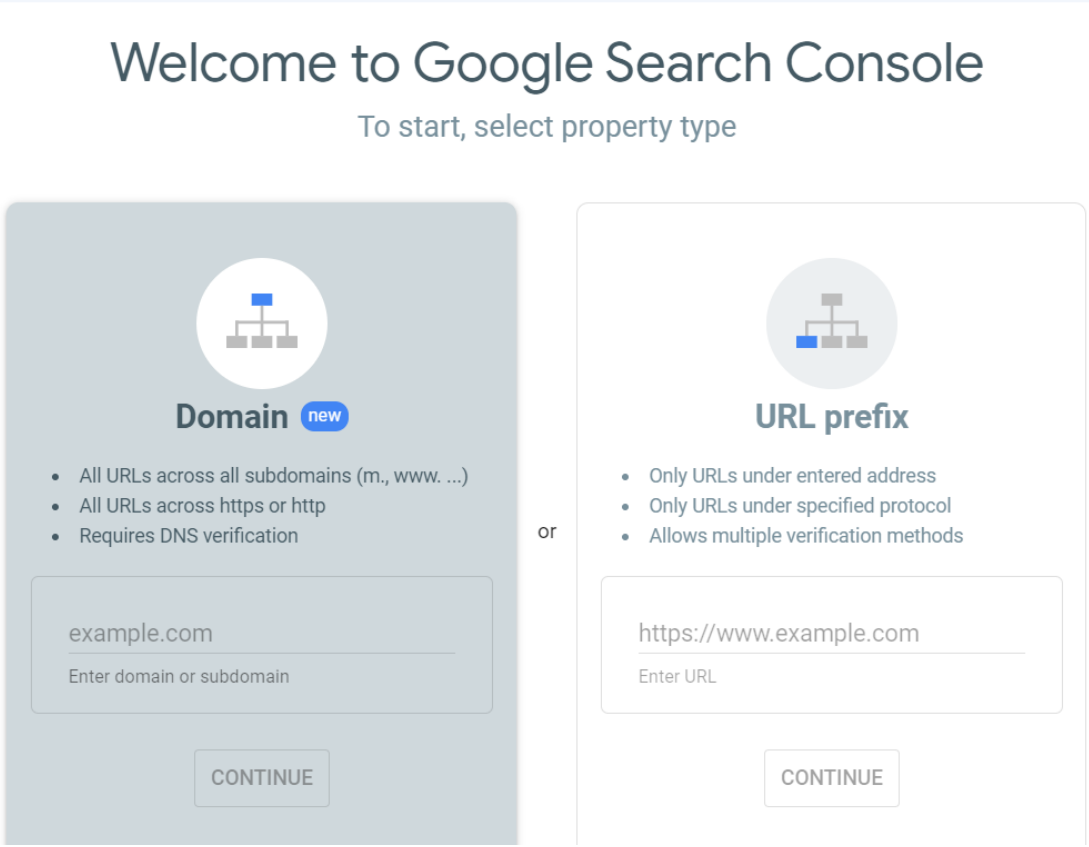


2. Hacer clic en el botón Comenzar ahora.

3. Iniciar sesión con su cuenta principal de Google o Gmail.

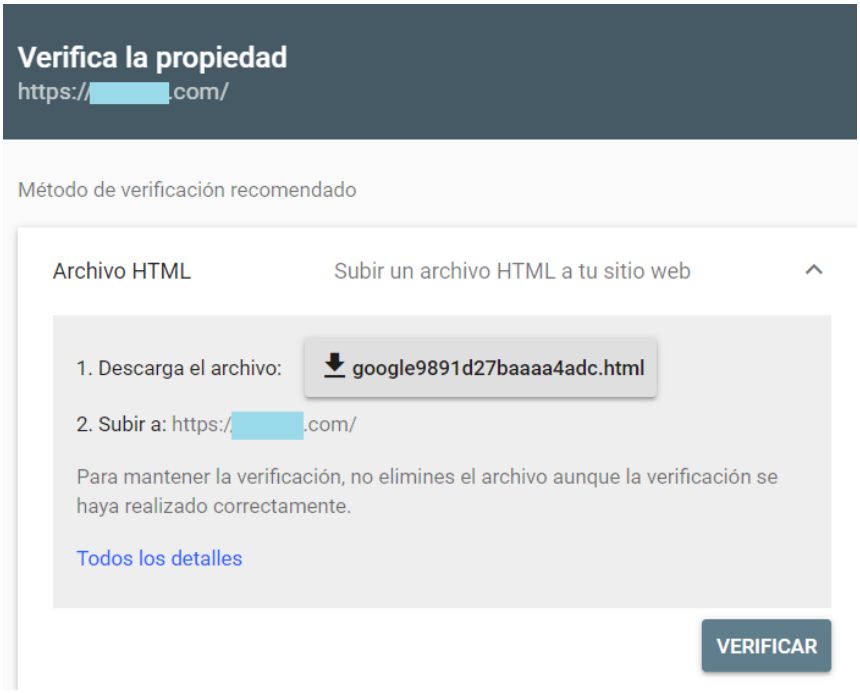


4. En el campo “Prefijo de URL”, ingresar la URL exacta de la página de inicio de su sitio web y hacer clic en Continuar. Asegúrese de incluir “http/https” y “www” según corresponda.

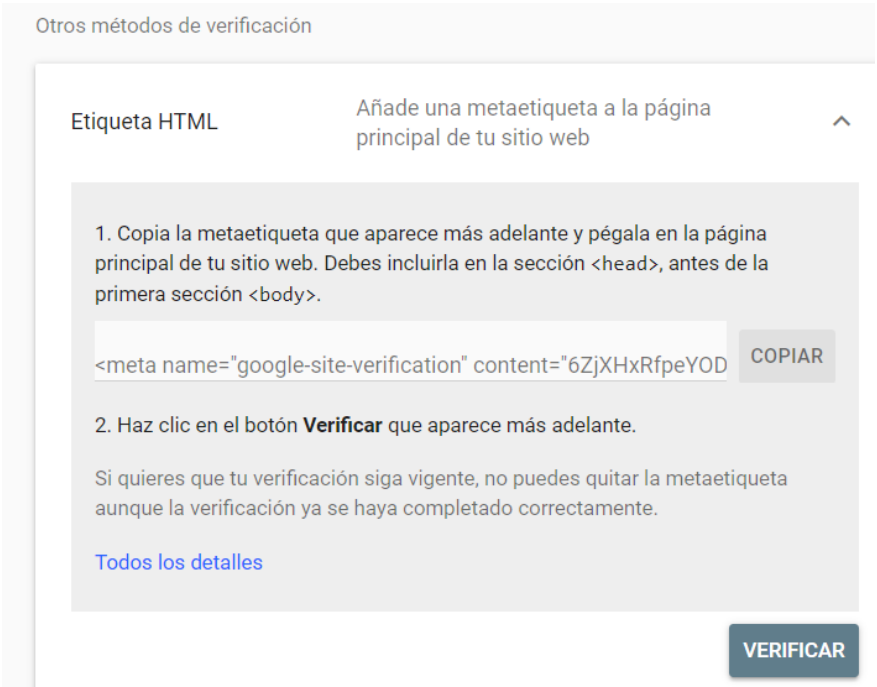


Una vez completados los pasos para agregar su sitio a Google Search Console, es necesario validar que realmente es el propietario del sitio web a través de algún de las siguientes verificaciones:

- Archivo HTML: Descargar el archivo que le provee Google y luego cargarlo a través de FTP u otro método a la raíz de su sitio web.

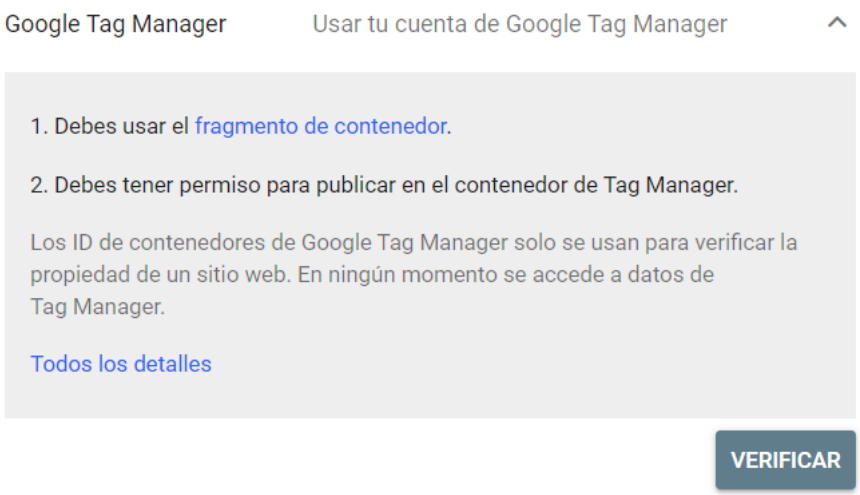


- Etiqueta HTML: Agregar una etiqueta HTML proveída al encabezado de su sitio.

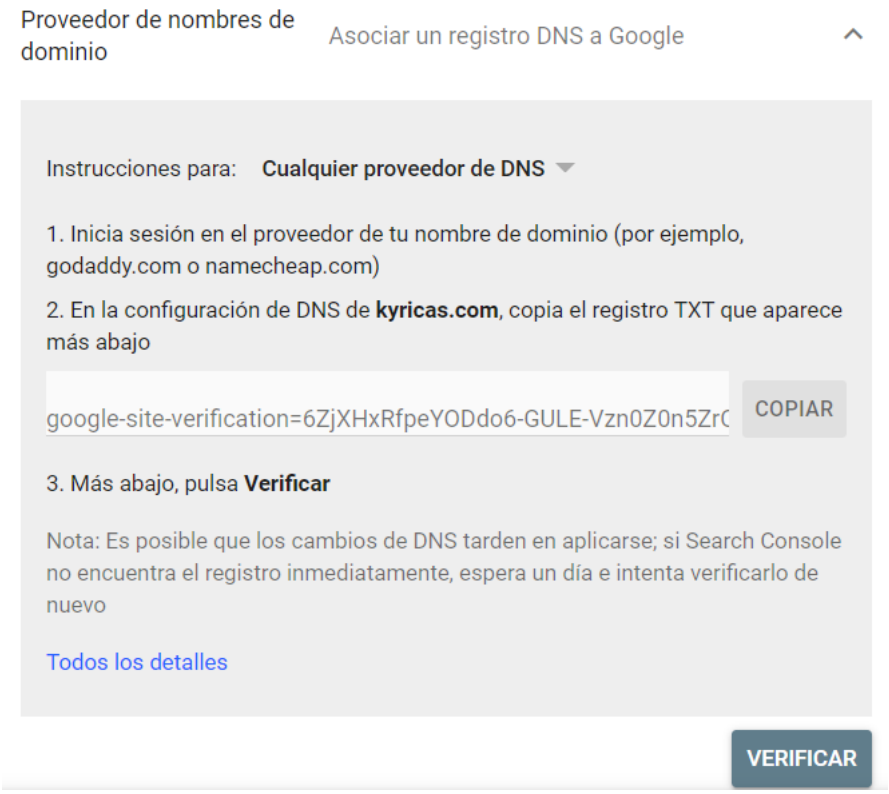


- Google Analytics: Realizar la verificación vinculando su cuenta de Google Analytics.

- Administrador de etiquetas de Google: Realizar la verificación vinculando su cuenta de Administrador de etiquetas de Google.

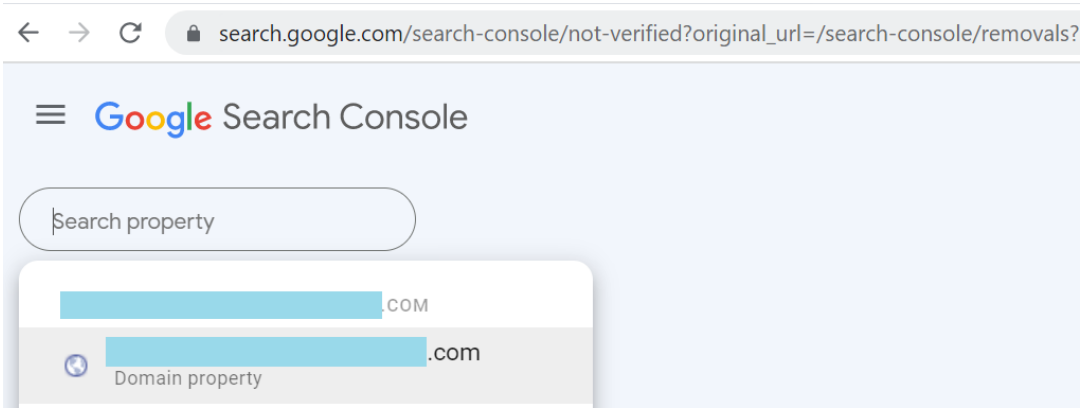


- Proveedor de nombre de dominio: Con esta opción, es necesario agregar un nuevo registro DNS a su cuenta de alojamiento web o proveedor de DNS.

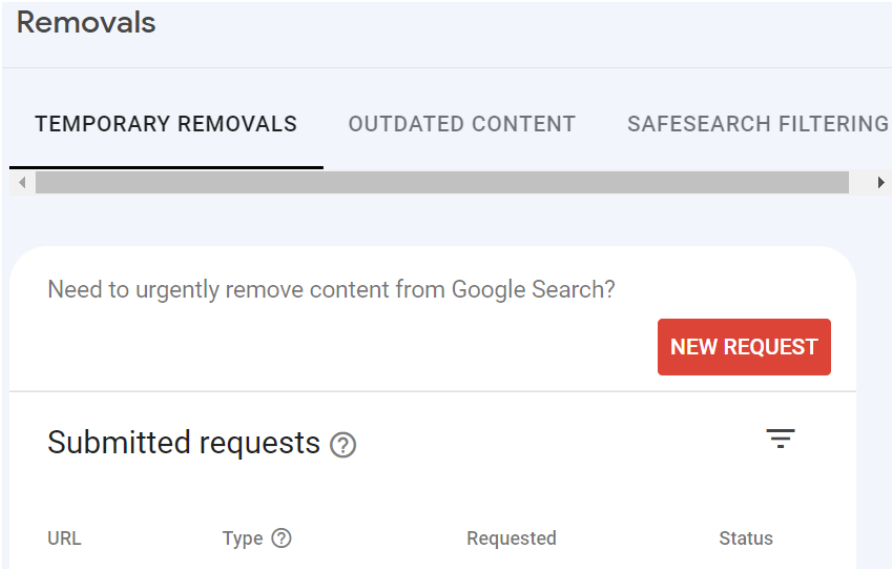


Una vez agregado correctamente su sitio en Google Search Console se deben seguir los siguientes pasos para eliminar la URL de las búsquedas de Google:

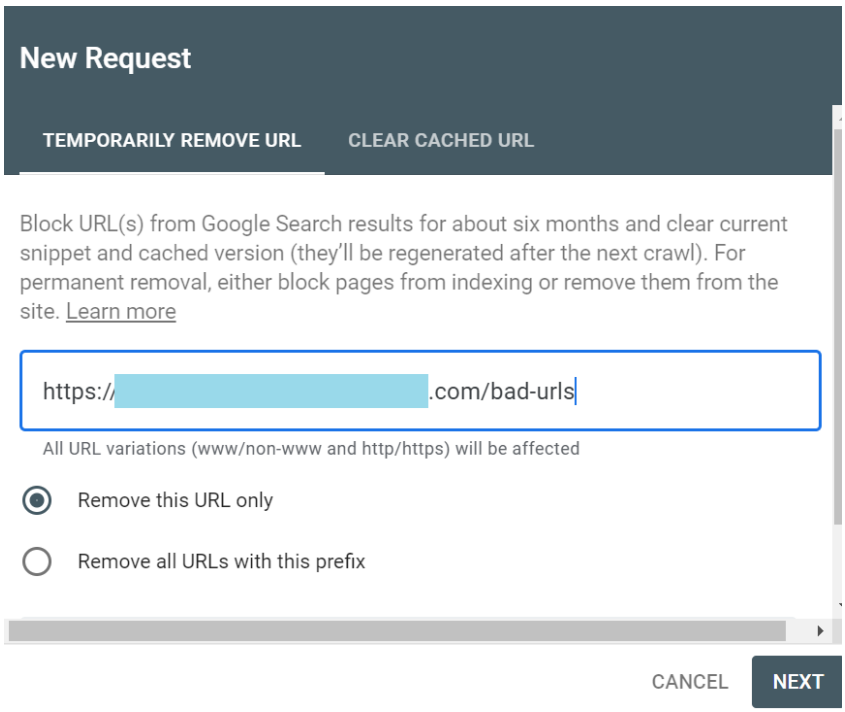
1. Visitar la herramienta Eliminar URL en el siguiente enlace.



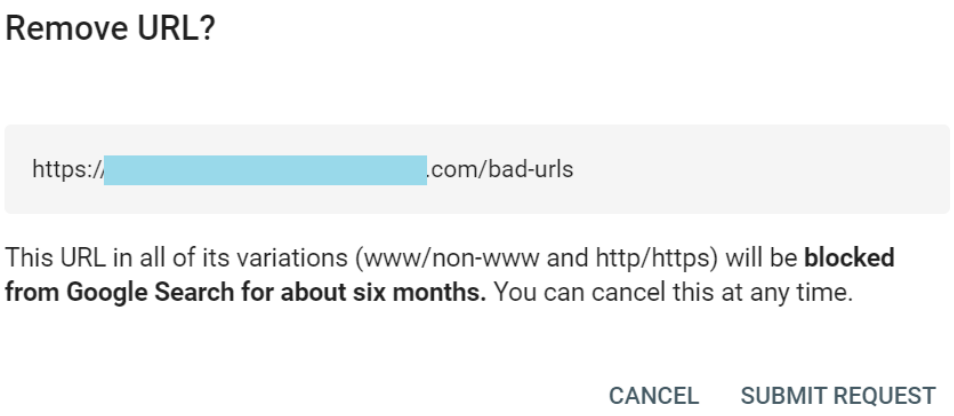
2. Seleccionar de la lista a partir del botón “Search property” el dominio del cual desea eliminar la URL.
3. En la pestaña “Temporary removals”, hacer click en el botón “NEW REQUEST”.



4. Ingresar la URL de su sitio que desea eliminar de los resultados de búsqueda de Google (Google por defecto bloqueará todas las URL incluyendo http/https, www y sin www como prefijo).



5. Elegir la opción “Remove this URL only” o “Remove all URLs with this prefix”, de acuerdo a su necesidad.
6. Confirmar su solicitud haciendo clic en el botón “SUBMIT REQUEST”.



Esto eliminará la URL de las búsquedas de Google durante aproximadamente 6 meses, así como del caché de Google.

Este método es sólo temporal, si la URL aún está activa en su sitio después de 6 meses es probable que Google la vuelva a agregar al índice y comience a mostrarla nuevamente en sus resultados de búsqueda.

Para el escenario 2 (comentarios SPAM en publicaciones del sitio WordPress) provocados por SPAM *bots* se describe a continuación la siguiente solución.

Escenario 2 - Cómo configurar sitio WordPress para evitar SPAM *bots* en comentarios de publicaciones

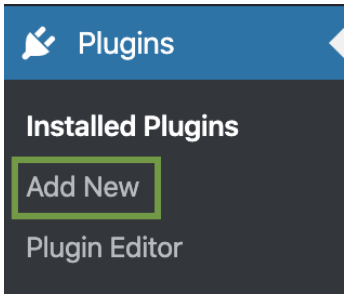
Una de las cosas que tanto molestan en un blog son los comentarios spam que llegan a cada artículo que se publica, estos en la mayoría de las veces llegan por medio de “*bots*”, llamados también “*spambots*“, dedicados a esta molesta tarea de visitar sitios en la red e intentar inyectar enlaces externos masivos de algun servicio, producto, texto, etc.

Estos *spambots* utilizan los formularios en de los sitios web para mandar el contenido, usualmente utilizan tecnologías OCR para resolver algunos tipos de CAPTCHAs, así que la utilización de los mismos no siempre es infalible.

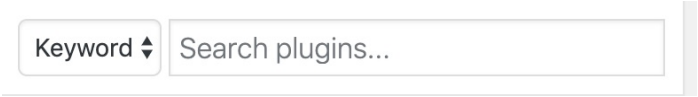
Afortunuadamente para los que utilizan WordPress como CMS existe un complemento o *plugin* llamado **Akismet**, que vendría como predeterminado en las instalaciones listo para su activación. Lo bueno de esta herramienta, además que atrapa gran cantidad de *spam*, es que, si se le escapa alguno, tiene la opción de marcación manual como spam y ayudaría a que **Akismet** "aprenda" de sus errores y aumente su efectividad.

¿Dónde configurarlo?

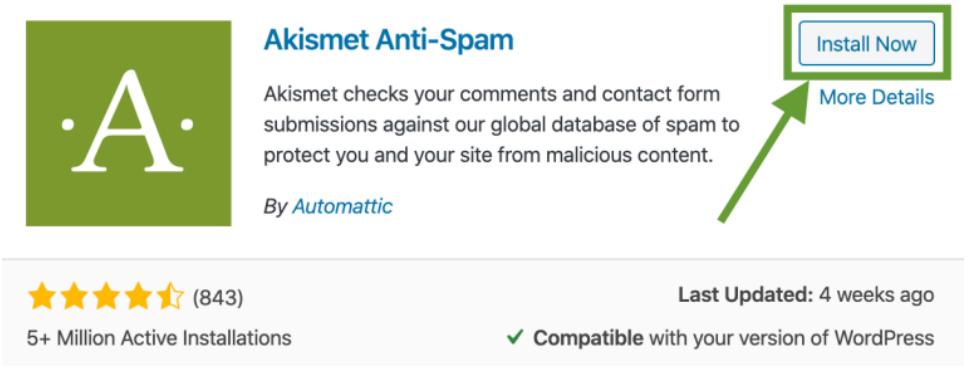
Primero debe ir al escritorio de administrador en WordPress, hasta la sección de *Plugins* en el menú principal y en el menú desplegable seleccionar *Add New*, si el plugin no se encuentra instalado por defecto.



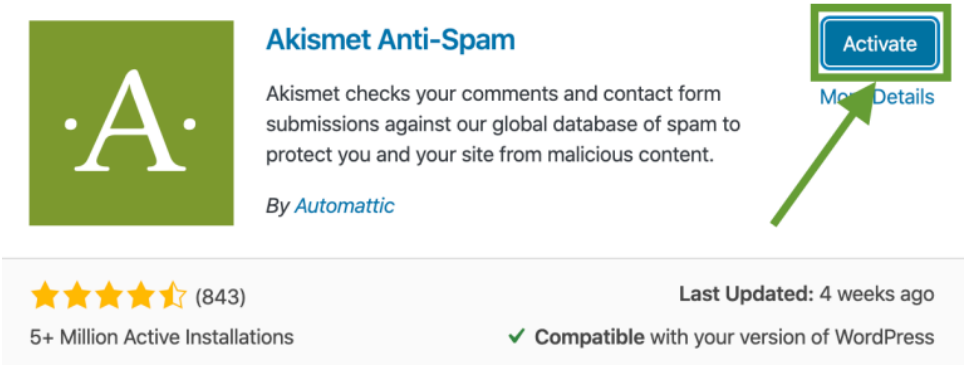
Se procede a buscar "**Akismet**" en la barra de búsqueda:



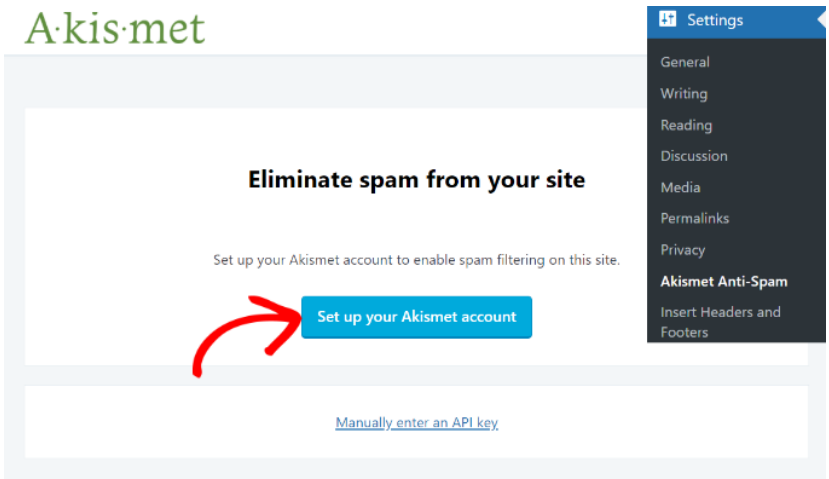
Se debe asegurar de que el autor del plugin sea “Automatic” y luego hacer clic en *Install Now:*



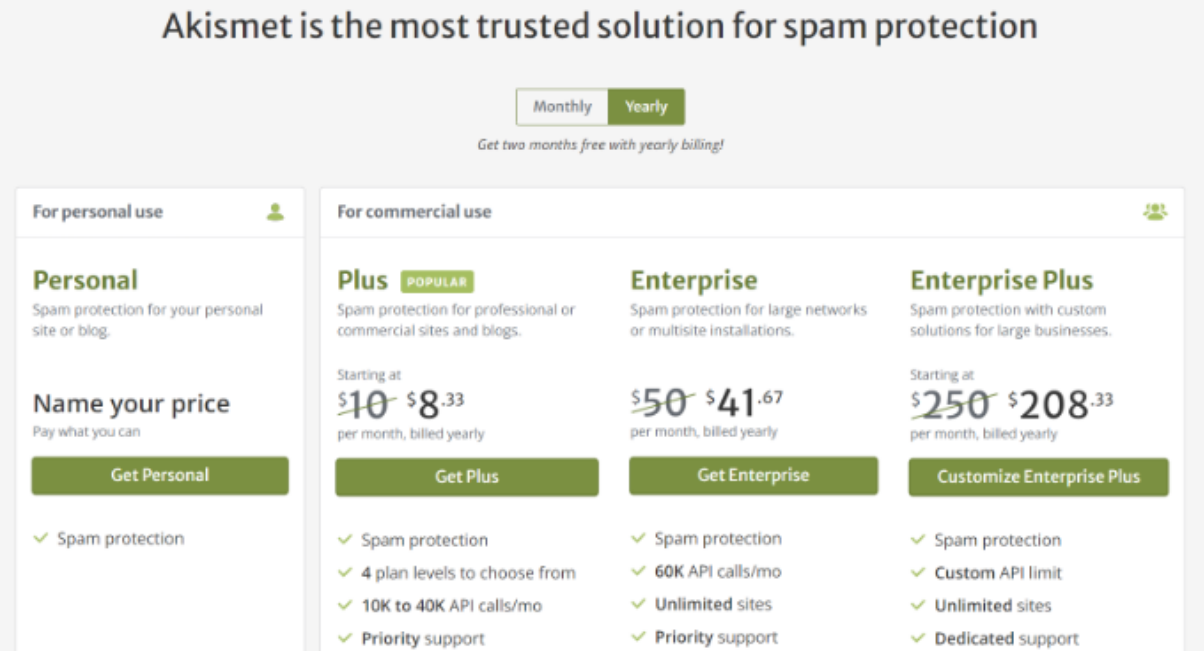
Una vez finalizada la instalación, se hace clic en el botón *Activate*:



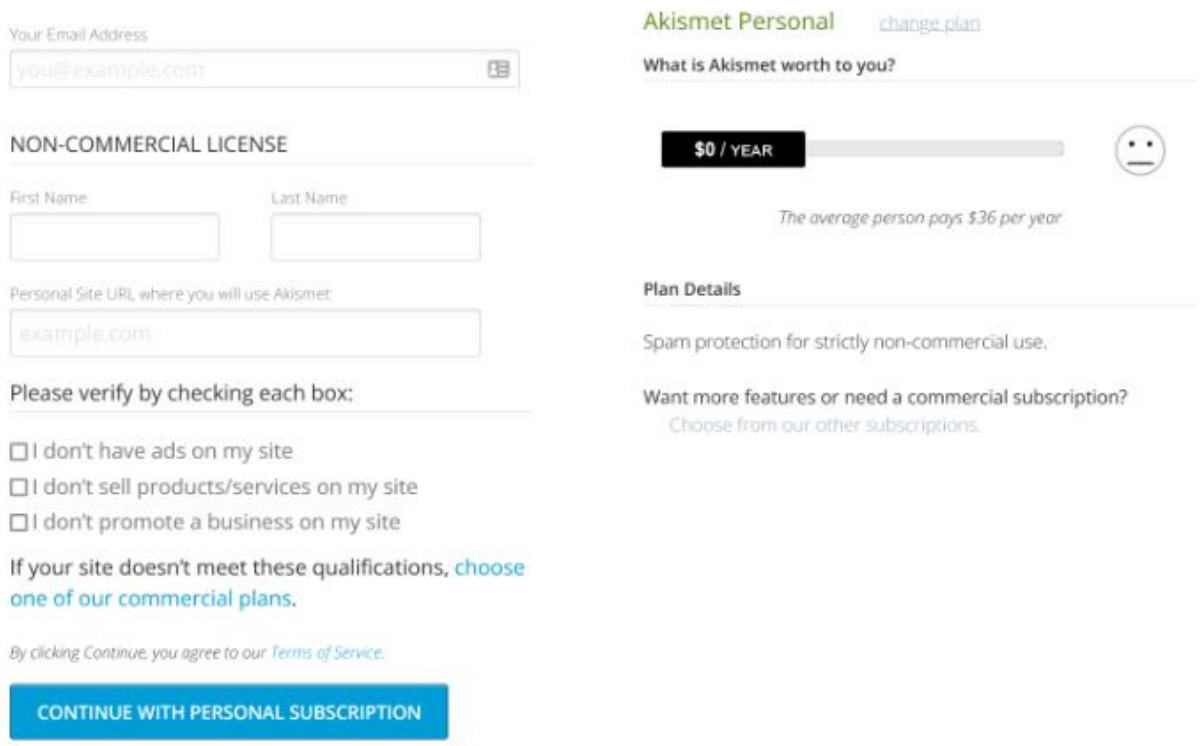
Es necesario conseguir una llave para utilizar esta API, haciendo clic en el botón azul para configurar una cuenta **Akismet**.



Se selecciona el tipo de plan, si es para un blog personal o para sitios comerciales de acuerdo al caso particular:



En la siguiente pantalla, deberá ingresar su dirección de correo electrónico, nombre y URL del sitio web para crear una cuenta, junto con elegir el precio que desea pagar por su cuenta. De forma predeterminada, el precio se establecerá en $ 36 por año.

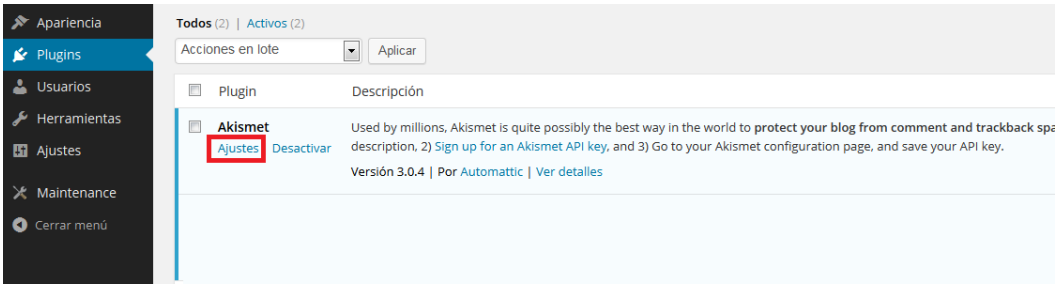


Sin embargo, puede mover el control deslizante de precios, a cualquier precio de 0 a $ 120 por año.

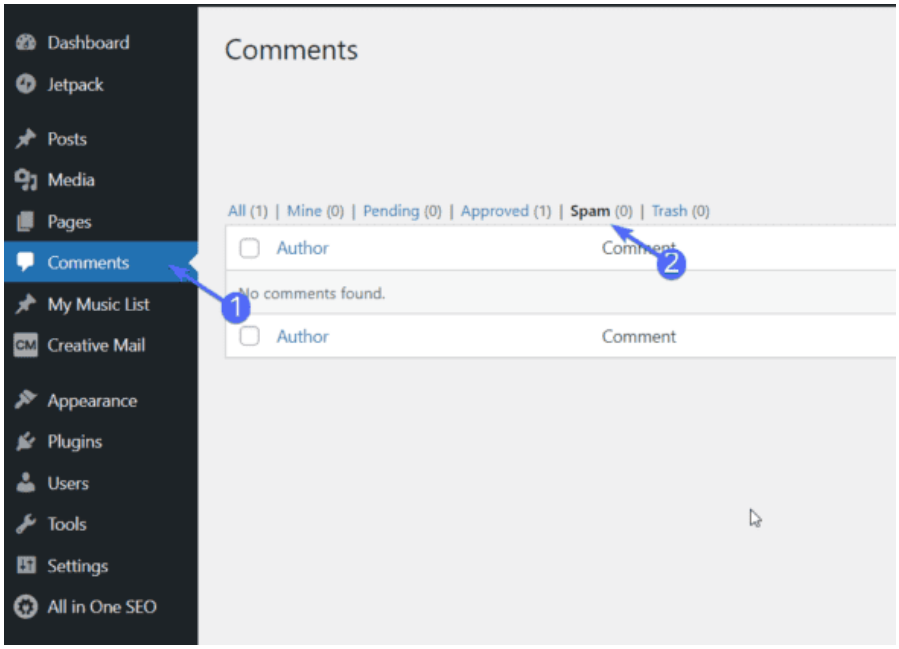
Aparte de eso, **Akismet** también le pedirá que marque las casillas si no está publicando anuncios, vendiendo productos y servicios, o promocionando un negocio en su sitio.

Una vez hecho esto, simplemente haga clic en el botón 'Continuar con la suscripción personal'. Usted recibirá por mail la confirmación del registro de su cuenta, así como la clave necesaria para activar **Akismet** en su sitio WordPress.

Finalmente, se procede a ingresar la clave en los ajustes de Akismet y para concluir hacer clic en “Ajustes”:



El *plugin* moverá cualquier comentario que detecte como spam a la sección "Spam" en el panel de WordPress. Para acceder a estos comentarios de *spam*, debe seleccionar *Comments -> Spam* en el panel de administración:



Escenario 3 - Cómo configurar sitio WordPress para evitar registro masivo de usuarios por SPAM *bots*

Para prevenir que *bots* realicen un registro masivo de usuarios en tu sitio WordPress hay una de serie de medidas a 8 posibles pasos a seguir cuya combinación es posible para alcanzar un mayor nivel de seguridad contra estos ataques:

1. Restricción del registro de usuarios en WordPress.
2. Establecimiento de un rol de usuario por defecto.
3. Verificación del registro de nuevos usuarios a través de correo electrónico.
4. Solicitudes de aprobación del administrador para cada nuevo registro.
5. Utilización de un formulario de registro seguro.
6. Utilización de un CAPTCHA.
7. Utilización de un reCAPTCHA.

8. Utiliza un *plugin* de prevención de *spam* de registros

¿Dónde configurarlo?

1. Restricción del registro de usuarios en WordPress.

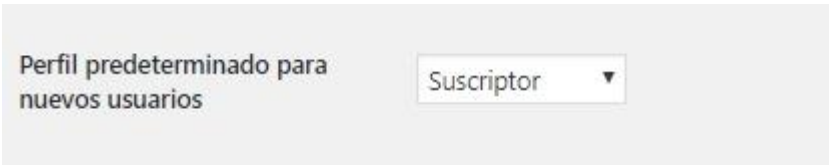
Primero, accede al backend de WordPress con tu usuario y contraseña.

Luego, ve a la sección, “Ajustes” -> “Generales” y asegúrate de tener desmarcada la opción “Cualquiera puede registrarse”.

2. Establecimiento de un rol de usuario por defecto.

Primero, accede al backend de WordPress con tu usuario y contraseña.

Luego, ve a la sección “Ajustes” –> “Generales” localiza la opción Perfil predeterminado para nuevos usuarios y, en el desplegable, selecciona la opción de Suscriptor.



Importante: Con esta opción estás aplicando una capa de seguridad, pero **no es suficiente para evitar el registro de usuarios spam**. Es necesario que tomes alguna otra medida adicional de las que te mostramos a continuación.

3. Verificación del registro de nuevos usuarios a través de correo electrónico.

Una buena opción para asegurarse de que todos los usuarios que se registran en tu web son legítimos, es aplicar una doble confirmación de registro a través de email. Eso podría lograrse un *plugin* como WPForms en su formato premium o User Registration como opción gratuita.

4. Solicitudes de aprobación del administrador para cada nuevo registro.

Al igual que en el caso anterior, puede lograrse a través de un *plugin* como User Registration que te permite hacerlo de manera gratuita. O bien WP Approve User también puede ser una buena alternativa.

Importante: Solo opta por esta opción cuando revises frecuentemente el backend de tu web y trabajes en ella frecuentemente. En caso contrario, dejar el registro pendiente durante varios días podría afectar a la experiencia de usuario de tu posible cliente.

5. Utilización de un formulario de registro seguro.

En este caso para conseguir esta funcionalidad, es necesario adquirir un *plugin* premium que pueda ofrecer de forma directa esta capa de seguridad. Por ejemplo, podrían ser WPForms o Gravity Forms.

6. Utilización de un CAPTCHA.

Puede lograrse fácilmente con el plugin Really Simple CAPTCHA se integra muy bien con plugins tan conocidos como Contact Form 7 y el desarrollador siempre lo mantiene al día.

7. Utilización de un reCAPTCHA.

Podemos decir que un sistema reCAPTCHA es la evolución del sistema que acabamos de ver en el apartado anterior.

Un sistema de acertijos o preguntas no siempre gusta a todos. Muchos administradores o usuarios prefieren opciones más simples, así que también disponen de una opción para ellos: el sistema reCAPTCHA.

Con esta opción los usuarios tan solo necesitan hacer “check” en una casilla de verificación. Muchos aseguran que este sistema mejora las conversiones y la experiencia de usuario web al hacer el proceso de verificación mucho más rápido.

Se puede obtener esta funcionalidad con los siguientes *plugins*:

- Google Captcha (reCAPTCHA)
- Advanced noCaptcha & invisible Captcha
- Login No Captcha reCAPTCHA

8. Utiliza un plugin de prevención de spam de registros

Tal y como podrías utilizar AKISMET (o alguna variante) para gestionar tus comentarios de WordPress, Stop Spammer Registration va a ayudarte a mantener los registros de tu web bajo control y banear automáticamente a los que se trata de puro spam.

Fuentes:

https://www.cert.gov.py/noticias/configuracion-de-wordpress-para-evitar-spam-bots-en-los-buscadores
https://www.cert.gov.py/application/files/1014/1685/0125/como_combatir_spam_en_wordpress.pdf
https://www.fixrunner.com/install-configure-akismet-plugin/
https://www.lucushost.com/blog/registro-de-usuarios-spam-wordpress/