



The screenshot shows the Sucuri website interface. At the top, there is a navigation bar with links for 'Website Monitoring', 'Website Firewall', 'Malware Removal', 'Knowledgebase', and 'Support'. The main content area features a large white box with the heading 'Free website malware and security checker'. Below the heading, there is a text input field containing 'example.com' and a 'Submit' button. A disclaimer is visible below the input field, stating that the scanner has limited access and results are not guaranteed. Below the disclaimer, there is a section titled 'Website protection you can depend on.' which includes three service cards: 'Website Monitoring' (Malware removal and hack repair), 'Website Firewall' (Protect and speed up), and 'Malware Removal' (Get rid of malware and clean up a...).

## Sucuri SiteCheck

*Sucuri SiteCheck es un escáner de seguridad remoto gratuito diseñado para propietarios de sitios web, administradores de sistemas y profesionales de IT que necesitan realizar inspecciones rápidas y no intrusivas. La herramienta analiza el código fuente externo para detectar infecciones de malware visibles, errores de configuración, estado en listas negras de Google o McAfee y software desactualizado en CMS como WordPress o Joomla, permitiendo un diagnóstico inmediato de la salud del dominio.*

[Visitar Sitio Oficial](#) [Preguntar a ChatGPT](#) [Preguntar a Claude](#) [Preguntar a Grok](#)

### Contenido del Dossier

- [Información de la Herramienta](#)
- [Consejos de Implantación](#)
- [Preguntas Frecuentes](#)
- [Contratos y Condiciones](#)

## INFORMACIÓN DE LA HERRAMIENTA

---

### Qué y para quién es

Sucuri SiteCheck es un escáner de seguridad remoto gratuito diseñado para realizar inspecciones rápidas y no intrusivas de sitios web. Su función técnica es analizar el código fuente externo (lado del cliente) para detectar infecciones visibles, errores de configuración y estado en listas negras. Está dirigido a propietarios de sitios web, administradores de sistemas y profesionales de seguridad que necesitan un diagnóstico inmediato sobre la salud superficial de un dominio sin necesidad de instalar software o acceder al servidor.

### Principal ventaja profesional

La capacidad de obtener un informe de seguridad consolidado en segundos que combina detección de malware, estado de indexación en múltiples autoridades de listas negras (como Google Safe Browsing o Norton) y verificación de software desactualizado, todo de forma externa y sin riesgo de afectar el rendimiento del sitio.

### Para quién no es

Profesionales que requieran una auditoría profunda a nivel de servidor (rootkit, backdoors ocultos en PHP o bases de datos) o empresas que busquen protección activa en tiempo real. Al ser un escáner remoto ("outside-in"), no puede detectar código malicioso que no se renderice en el navegador del visitante.

### funcionalidades clave

- Detección de malware remoto: Identifica scripts maliciosos, inyecciones de IFRAME y redirecciones sospechosas en el HTML/JS visible.
- Monitor de Listas Negras (Blacklist Check): Verifica si el dominio está penalizado por Google, McAfee, PhishTank, Yandex y otras entidades.
- Auditoría de Software: Detecta versiones obsoletas de CMS (WordPress, Joomla, Magento, Drupal) y plugins vulnerables.
- Verificación de Seguridad de Red: Revisa el estado de certificados SSL y posibles errores de configuración en el servidor web.
- Detección de Spam SEO: Encuentra enlaces ocultos o palabras clave inyectadas que afectan el posicionamiento en buscadores.

### Precios

La herramienta SiteCheck como tal es gratuita, aunque forma parte del ecosistema de captación para la plataforma de pago de Sucuri.

- Versión gratuita: Escaneo manual ilimitado a través de la web, proporcionando un informe detallado pero únicamente de la parte pública del sitio.
- Rango de precios (Plataforma completa): Desde aprox. 190€ hasta 460€ al año por sitio (facturación anual).
- Versiones de pago (Sucuri Platform): Incluyen limpieza de malware ilimitada por expertos, Firewall (WAF), escaneo a nivel de servidor (FTP/SFTP) y monitorización automática cada 30-60 minutos.

### Perfil del usuario

- Agencias de marketing y mantenimiento web que necesiten validar rápidamente la seguridad de un cliente potencial.
- Departamentos de IT para verificaciones de rutina tras despliegues.
- Freelance especializados en WordPress o e-commerce que gestionen múltiples sitios.
- Especialistas en SEO para diagnosticar caídas repentinas de tráfico debidas a penalizaciones de seguridad.

### Nivel técnico requerido

- Nivel técnico para su uso: Muy bajo. Basta con introducir la URL en el navegador.
- Nivel técnico para su configuración: No requiere instalación.
- Conocimientos necesarios: Comprensión básica de seguridad web (conceptos como malware, SSL o CMS) para interpretar los resultados del informe.

### Ejemplos de uso profesional

- Auditoría rápida previa a la contratación de un servicio de mantenimiento web.
- Verificación de emergencia cuando un sitio web muestra alertas de "sitio no seguro" en Google Chrome.
- Comprobación de la correcta implementación de las cabeceras de seguridad y el certificado SSL tras una migración.

- Detección de inyecciones de spam que no son visibles a simple vista pero afectan al SEO.

#### Uso y distribución

- Versión web: Acceso directo desde cualquier navegador.
- Extensión del navegador: Disponible para Google Chrome.
- Extensiones CMS: Integrado en el plugin oficial de Sucuri para WordPress.
- Widget: Dispone de un widget embebible para que otras webs ofrezcan el servicio de escaneo.

#### Integraciones

- Facilidad de integración: Alta (vía plugin o API en versiones de pago).
- API propia: Sucuri ofrece una API para clientes de pago que permite automatizar los escaneos e integrar los reportes en dashboards propios.
- Plugins nativos: Integración profunda con WordPress, permitiendo ver los informes de SiteCheck directamente en el escritorio del CMS.

#### Notas finales

información legal, licencias, contratos

- El uso de la herramienta gratuita está sujeto a los términos de servicio de Sucuri (GoDaddy Group). La herramienta no garantiza la detección del 100% del malware dado que es un escaneo remoto. La propiedad intelectual de los informes pertenece a Sucuri, aunque los resultados son de libre consulta para el usuario que realiza el escaneo.

#### Para más información:

- Sitio web oficial: <https://sitecheck.sucuri.net>
- Precios y planes: <https://sucuri.net/pricing>
- Documentación técnica: <https://docs.sucuri.net>
- Twitter: [https://twitter.com/sucuri\\_security](https://twitter.com/sucuri_security)

## CONSEJOS DE IMPLANTACIÓN

---

### Aplicación profesional

- Empresas y perfiles: Agencias de desarrollo web, departamentos de IT de PYMES, especialistas en SEO, consultores de ciberseguridad y administradores de e-commerce.
- Presupuesto: El recurso de análisis es gratuito y sin coste por ejecución. Los planes de mitigación y firewall profesional oscilan entre 199 USD y 499 USD anuales por sitio web.
- Puntos clave: Diagnóstico rápido de reputación de dominio, verificación visual de inyecciones de código y auditoría técnica de cabeceras de seguridad sin impacto en el servidor.

### Madurez digital requerida

- Usuarios: Nivel básico para ejecutar el escaneo; nivel intermedio (webmaster) para interpretar y corregir las vulnerabilidades de software o configuraciones de servidor detectadas.
- Empresa: Nivel inicial. No requiere infraestructura propia ni procesos complejos de implementación, al tratarse de un recurso de uso externo.

### Plan orientativo de implantación

#### Pasos necesarios y estimaciones

- Tiempos estimados de despliegue: Inmediato (acceso vía navegador).
- Evaluación inicial: Identificación de los activos web críticos que deben ser auditados periódicamente.
- Ejecución de prueba de concepto: Realización de un escaneo inicial para establecer una línea base de la salud de seguridad de la web.
- Integración en flujo de trabajo: Establecer el uso de SiteCheck como paso obligatorio tras cada actualización de CMS o plugins.
- Seguimiento: Revisión de los informes de listas negras para asegurar la entregabilidad de correos y el posicionamiento SEO.

### Necesidades de formación del equipo

- Capacitación en interpretación de errores de seguridad web (XSS, inyecciones JS, errores de certificados SSL).
- Formación en la identificación de falsos positivos y comprensión de las limitaciones del escaneo remoto frente al escaneo de nivel de servidor.

### Perfiles necesarios

- Perfiles técnicos necesarios: Desarrollador web o administrador de sistemas para aplicar los parches recomendados por la herramienta.
- Otros: Un responsable de SEO para monitorizar el estado de las listas negras de Google y otros motores de búsqueda.

### Retorno de la inversión

- Tiempos: Ahorro inmediato en tiempo de diagnóstico manual, reduciendo horas de consultoría técnica de seguridad.
- KPIs: Reducción del tiempo de respuesta ante infecciones (Mean Time to Detect), número de incidencias por software desactualizado y estado de permanencia en "listas blancas" de navegación segura.

### Otros

- Limitaciones técnicas: Al ser un escáner "outside-in", no detecta troyanos a nivel de sistema operativo, procesos maliciosos en ejecución en memoria del servidor ni vulnerabilidades en bases de datos que no se reflejen en el renderizado HTML.
- Complementariedad: Se recomienda su uso conjunto con el plugin gratuito de Sucuri para WordPress para añadir una capa de auditoría de logs y cambios en el sistema de archivos local.
- Propiedad y respaldo: La herramienta pertenece a Sucuri, empresa propiedad de GoDaddy, lo que garantiza una base de datos de firmas de malware actualizada constantemente.

## PREGUNTAS FRECUENTES

---

### ¿Qué es Sucuri SiteCheck y cuál es su alcance técnico?

Sucuri SiteCheck es un escáner de seguridad remoto y gratuito que analiza la capa externa de un sitio web (lado del cliente). Su función principal es inspeccionar el código fuente HTML, archivos JavaScript y cabeceras HTTP para identificar anomalías visibles, malware conocido, errores de configuración y el estado de reputación en listas negras.

### ¿Cuál es la diferencia entre el escaneo gratuito y la plataforma de pago?

El escaneo gratuito es una auditoría externa de tipo 'outside-in' que solo detecta lo que un navegador puede ver. La plataforma de pago incluye escaneos a nivel de servidor (vía FTP/SFTP) para detectar backdoors ocultos en PHP o bases de datos, además de ofrecer un Firewall de Aplicaciones Web (WAF) y servicios de limpieza profesional de malware.

### ¿Es capaz de detectar el 100% de las amenazas en un sitio web?

No. Al ser un escáner remoto, no tiene acceso a los archivos internos del servidor ni a la base de datos. Por lo tanto, no puede detectar scripts maliciosos que solo se ejecutan en el servidor, troyanos a nivel de sistema operativo o vulnerabilidades lógicas complejas que no se reflejen en el código de salida.

### ¿Cómo ayuda esta herramienta en el cumplimiento normativo y privacidad?

Ayuda a verificar la implementación de certificados SSL/TLS y cabeceras de seguridad, elementos críticos para la integridad de los datos según normativas como el RGPD. No obstante, el escaneo es puramente técnico y no sustituye a una auditoría legal o de cumplimiento de privacidad exhaustiva.

### ¿Es Sucuri SiteCheck una herramienta de código abierto (Open Source)?

No, es una tecnología propietaria desarrollada por Sucuri (propiedad de GoDaddy). Aunque ofrece un plugin gratuito para WordPress y herramientas de acceso público, el motor de detección y las bases de datos de firmas de malware son cerradas y gestionadas por la empresa.

### ¿Qué entidades se consultan para el Monitor de Listas Negras?

La herramienta contrasta el dominio con múltiples bases de datos de autoridades de seguridad, incluyendo Google Safe Browsing, Norton Safe Web, PhishTank, Opera, SiteAdvisor (McAfee) y Yandex, para verificar si el tráfico del sitio está siendo bloqueado o advertido.

### ¿Cuál es el coste de las soluciones profesionales de Sucuri?

Aunque el escáner SiteCheck es gratuito, las soluciones de protección y respuesta ante incidentes tienen un rango de precios que oscila aproximadamente entre los 190€ y 460€ anuales por sitio web, dependiendo de la frecuencia de escaneo y los tiempos de respuesta garantizados.

### ¿Qué impacto tiene el escaneo en el rendimiento del servidor?

El impacto es prácticamente inexistente. El escáner funciona realizando peticiones HTTP similares a las de un usuario estándar o un bot de búsqueda, por lo que no consume recursos significativos del servidor ni requiere la instalación de agentes que puedan degradar la velocidad.

### ¿Puede integrarse en flujos de trabajo automatizados?

Sí, para usuarios profesionales y clientes de pago, Sucuri ofrece una API que permite automatizar las consultas de escaneo. También existen integraciones nativas mediante plugins para CMS como WordPress, facilitando la monitorización desde el panel de administración.

### ¿Es seguro utilizar este escáner en cualquier sitio web?

Sí, es una tecnología segura y no intrusiva. No intenta explotar vulnerabilidades ni realizar pruebas de penetración agresivas; simplemente lee e interpreta la información pública del sitio para informar sobre posibles riesgos de seguridad.



## CONTRATOS Y CONDICIONES

---

### Principales recomendaciones

- Realice los escaneos únicamente sobre dominios de su propiedad o sobre los que tenga autorización expresa, ya que el escaneo automatizado sin consentimiento podría interpretarse como una actividad de reconocimiento no autorizada.
- No introduzca URLs que contengan parámetros con datos personales o tokens de sesión en el buscador, ya que estos datos podrían quedar registrados en los sistemas de Sucuri (GoDaddy).
- Utilice esta herramienta solo como una primera capa de diagnóstico superficial; el cumplimiento normativo en seguridad requiere auditorías internas más profundas que SiteCheck no puede realizar.
- Si gestiona sitios de clientes, informe a estos de que utiliza servicios de terceros (Sucuri/GoDaddy) para las comprobaciones de salud del sitio en sus contratos de mantenimiento.

### Privacidad y protección de datos

- Responsabilidades: Sucuri (propiedad de GoDaddy) actúa como un prestador de servicios independiente al realizar el escaneo. La empresa española es responsable de no exponer URLs sensibles que contengan datos de carácter personal.
- Ubicación de los datos: Los datos de los escaneos y la infraestructura de Sucuri se encuentran principalmente en Estados Unidos. Al ser una empresa del grupo GoDaddy, se rigen por sus políticas globales de privacidad.
- Transferencia internacional: El uso de SiteCheck implica una transferencia de datos (dirección IP del solicitante y URL consultada) hacia servidores fuera de la Unión Europea. GoDaddy utiliza Cláusulas Contractuales Tipo (SCC) para legitimar este flujo de datos conforme al RGPD.
- Derechos ARCO: Los usuarios pueden ejercer sus derechos de acceso, rectificación, supresión y oposición a través de los canales de privacidad globales de GoDaddy.

### Propiedad intelectual

- Propiedad de datos: El usuario conserva la propiedad de su sitio web, pero el informe de diagnóstico generado, su estructura y la base de datos de firmas de malware son propiedad intelectual de Sucuri.
- Propiedad del resultado/procesamiento: Los resultados del escaneo son para uso informativo del usuario. No está permitida la reventa de estos informes gratuitos ni su extracción masiva (scraping) para incluirlos en productos comerciales propios sin licencia de API específica.

### Usos y prohibiciones

- Usos prohibidos: No se permite el uso de la herramienta para realizar ataques de denegación de servicio (DoS) mediante escaneos masivos, ni el uso de scripts automatizados para consultar el escáner gratuito sin autorización. Está prohibido intentar realizar ingeniería inversa sobre el motor de detección de SiteCheck.
- Usos admitidos: Diagnóstico puntual de infecciones de malware, verificación de estado de listas negras y comprobación de certificados SSL para mantenimiento preventivo.

### Seguridad y certificaciones

- Seguridad: La herramienta utiliza un método de escaneo "No-Intrusivo", lo que significa que solo analiza lo que un navegador o un bot de búsqueda vería, sin interactuar con los archivos internos del servidor.
- Certificaciones: GoDaddy (matriz de Sucuri) cuenta con certificaciones internacionales de seguridad de la información, aunque el servicio gratuito SiteCheck no emite un certificado de cumplimiento de seguridad válido para normativas como PCI-DSS.

### Otros

- Impacto legal: Bajo. Al ser un escáner externo que no requiere instalación en los sistemas de la empresa, el riesgo legal es mínimo siempre que no se procesen URLs con datos personales.
- Limitación de responsabilidad: Sucuri declina cualquier responsabilidad legal por falsos negativos (malware no detectado) o falsos positivos que puedan afectar a la reputación de la empresa española.

### Fuentes consultada:

- [Términos de servicio de Sucuri](#)
- [Política de privacidad de GoDaddy y Sucuri](#)
- [Documentación técnica de SiteCheck](#)
- [Centro de confianza de GoDaddy](#)

**Para más información y herramientas:**

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

[Inicio](#) [Todas las herramientas](#) [Categorías](#)

Este documento ofrece recomendaciones generadas mediante análisis humano y sistemas de IA automatizados. La información tiene carácter meramente informativo y no constituye asesoramiento legal, profesional ni garantía de resultados. Las marcas, logotipos y nombres comerciales pertenecen a sus respectivos propietarios y se utilizan únicamente con fines identificativos.