

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.birrata.es/	Checks	9 pruebas
Dominio	www.birrata.es	Hallazgos	44 totales
Fecha	25 de septiembre de 2026 a las 12:42	Problemas	2 detectados

A

94/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar una auditoría de seguridad pasiva, el sitio web presenta un nivel de protección sobresaliente con una puntuación de 94/100 y una calificación de A. El análisis ejecutó un total de 9 comprobaciones pasivas, de las cuales 7 resultaron conformes y 2 generaron advertencias técnicas menores. No se registraron fallos críticos ni vulnerabilidades de alta prioridad durante el escaneo. Se concluye que el sitio es seguro para su uso actual, aunque requiere ajustes en la gestión de recursos externos y archivos de rastreo para alcanzar la optimización total.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
89 dias restantes (expira: 2026-12-23T17:15:03.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-09-24T17:15:04.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
Server: Vercel — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-...
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=63072000
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(), payment=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 308 redirige a https://www.birrata.es/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- INFO

Tecnologias detectadas
React, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)

● INFO **Version CMS**
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK
No se encontraron cookies

● INFO **Cookies detectadas**
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO
1 recurso(s) HTTP en pagina HTTPS

● MEDIO **Recurso HTTP (href (link/stylesheet))**
http://localhost:3000

Robots.txt y Sitemap — 60/100

Estado: AVISO
Falta robots.txt

● INFO **sitemap.xml**
Presente, 82 URLs

● BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK
2 puerto(s) abierto(s), todos esperados

● INFO **Puerto 21 (FTP)**
Cerrado — Transferencia de archivos sin cifrar

● INFO **Puerto 22 (SSH)**
Cerrado — Acceso remoto seguro

● INFO **Puerto 23 (Telnet)**
Cerrado — Acceso remoto sin cifrar

● INFO **Puerto 25 (SMTP)**
Cerrado — Envio de correo

● INFO **Puerto 80 (HTTP)**
Abierto (esperado) — Servidor web

● INFO **Puerto 443 (HTTPS)**
Abierto (esperado) — Servidor web seguro

● INFO **Puerto 3306 (MySQL)**
Cerrado — Base de datos MySQL expuesta

● INFO **Puerto 3389 (RDP)**
Cerrado — Escritorio remoto Windows

● INFO **Puerto 5432 (PostgreSQL)**
Cerrado — Base de datos PostgreSQL expuesta

● INFO **Puerto 6379 (Redis)**
Cerrado — Cache Redis sin autenticacion por defecto

● INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy

● INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[MEDIA] Contenido mixto: Se detectó un recurso vinculado mediante el protocolo HTTP (http://localhost:3000), lo cual es peligroso porque puede causar errores de carga en el navegador y exponer el entorno de desarrollo.

[BAJA] Cabecera de servidor expuesta: La respuesta del servidor revela el uso de Vercel, lo cual es peligroso ya que facilita a un atacante potencial el reconocimiento de la infraestructura y la búsqueda de exploits específicos.

[BAJA] Ausencia de archivo robots.txt: La falta de este archivo impide definir reglas de navegación para motores de búsqueda, lo que podría derivar en el rastreo involuntario de directorios sensibles.