

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://conectayaentuhogar.es
Dominio conectayaentuhogar.es
Fecha 19 de junio de 2026 a las 20:39

Checks 9 pruebas
Hallazgos 45 totales
Problemas 3 detectados

A

94/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha arrojado una puntuación final de 94/100, lo que equivale a una nota A. Se han ejecutado un total de 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 advertencias, sin detectarse fallos críticos en la infraestructura. Los resultados demuestran un compromiso sólido con la seguridad de la información, especialmente en lo que respecta al cifrado de datos y la configuración de cabeceras. Aunque no se ejecutó un pentest activo para probar defensas en tiempo real, las pruebas pasivas confirman que el sitio es seguro para el usuario final. Se recomienda atender las advertencias menores para alcanzar la excelencia en la postura de seguridad.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 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 42 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
42 dias restantes (expira: 2026-07-31T16:04:25.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-02T16:04:26.000Z
- 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: hcdn — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: Next.js — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**
Presente: upgrade-insecure-requests
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains; preload
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **INFO** **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=(), interest-cohort=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://conectayaentuhogar.es/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=31536000 (365 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, 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 (src (script/img/iframe))**
http://localhost:8400/live.js

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
Presente, 115 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

[MEDIUM] Contenido Mixto: Se detectó la carga del recurso http://localhost:8400/live.js a través de una conexión no segura, lo que puede permitir ataques de degradación de seguridad o inyecciones de script.

[LOW] Falta de archivo robots.txt: La ausencia de este archivo impide definir directrices de indexación para rastreadores, lo que afecta la visibilidad y el control del contenido.

[LOW] Server header expuesto: La cabecera Server revela el valor hcdn, facilitando a posibles atacantes información sobre la infraestructura de entrega de contenido.

[LOW] X-Powered-By expuesto: La cabecera revela el uso de Next.js, lo que permite a un actor malintencionado identificar el framework y buscar vulnerabilidades específicas para dicha tecnología.