# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://juego-descargar.com/football-manager-2020-para-pc-espanol/ | Checks | 9 pruebas |
| Dominio | juego-descargar.com | Hallazgos | 44 totales |
| Fecha | 30 de abril de 2026 a las 00:19 | Problemas | 13 detectados |

**C**

62/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 62/100, lo que resulta en una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 se identificaron como fallos críticos. Aunque la infraestructura básica de cifrado es correcta, existen deficiencias severas en las políticas de seguridad del servidor y la exposición de información técnica sensible. En su estado actual, el sitio se considera vulnerable a ataques de interceptación, inyección de código y explotación de software desactualizado.

## Resumen de Riesgos

| 0 | 5 | 6 | 2 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 52 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress |
| Version CMS Expuesta | 20 | FALLO | WordPress 6.9.4 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 60 | AVISO | Falta robots.txt |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 8080 (HT... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 52 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-06-20T21:15:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-22T20:17:22.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://juego-descargar.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

## Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

## 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

## Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

## Analisis de Seguridad

**VULNERABILIDADES DETECTADAS**

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: No hay protección contra clickjacking, lo que permite que el sitio sea cargado en frames externos para engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo posibles degradaciones a HTTP.
[HIGH] Versión de WordPress expuesta: Se detectó la versión 6.9.4 públicamente, lo que facilita a atacantes la búsqueda de CVEs y exploits conocidos.

[MEDIUM] X-Content-Type-Options: Al no estar configurada, el sitio queda expuesto a ataques de sniffing de tipos MIME.
[MEDIUM] Referrer-Policy: La falta de control sobre la información de referencia puede filtrar datos de navegación a dominios de terceros.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso a APIs sensibles del navegador como la cámara, micrófono o geolocalización.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor alternativo o proxy expuesto aumenta la superficie de ataque del servidor.
[MEDIUM] Archivo /readme.html expuesto: Este documento accesible revela detalles técnicos sobre la instalación y versión del CMS.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible para cualquier usuario, permitiendo ataques de fuerza bruta dirigidos.
[LOW] HSTS no configurado: Aunque el sitio redirige a HTTPS, no existe una instrucción persistente de seguridad para el navegador.
[LOW] Cabecera Server expuesta: El valor "cloudflare" revela información sobre la infraestructura de red utilizada.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso de WordPress 6.9.4, facilitando la fase de reconocimiento de un ataque.
[LOW] Falta de archivo robots.txt: No se han definido reglas de rastreo, lo que puede llevar a la indexación de directorios no deseados.