EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.coca-cola.com/pe/es	Checks	9 pruebas
Dominio	www.coca-cola.com	Hallazgos	50 totales
Fecha	31 de julio de 2026 a las 22:51	Problemas	6 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

La evaluación de seguridad realizada al sitio web arroja una puntuación de 89/100, lo que corresponde a una calificación de nota B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo como resultado 7 verificaciones exitosas, una advertencia y un fallo en la configuración de cabeceras. La infraestructura presenta un cifrado de transporte robusto y una gestión de redirecciones adecuada. No obstante, se identificaron debilidades en la protección contra ataques de clic y en la seguridad de las cookies. En conclusión, el sitio es mayormente seguro, pero vulnerable a ataques técnicos específicos que podrían comprometer la integridad de la sesión del usuario.

Resumen de Riesgos

0	2	2	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 152 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
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	67	AVISO	country_region_code: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 152 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  152 dias restantes (expira: 2026-12-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-16T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src * data: mediastream: blob: filesystem: about: ws: wss: 'unsafe-eval'...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.coca-cola.com/
- 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**
  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 — 67/100

Estado: AVISO

country_region_code: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: country_region_code — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: country_region_code — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: country_region_code — SameSite**
  SameSite=strict

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (184 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.coca-cola.com/content/onexp.sitemap-index.xml
- 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

[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes) externos, facilitando ataques de clickjacking.
[HIGH] Cookie country_region_code: Esta cookie carece del atributo HttpOnly, lo que permite su acceso mediante scripts y eleva el riesgo de robo de sesión via XSS.
[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que podría provocar la filtración involuntaria de información de navegación a sitios de terceros.
[MEDIUM] Permissions-Policy: La falta de esta configuración impide restringir el uso de APIs sensibles del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el valor CEP, proporcionando pistas innecesarias sobre la tecnología subyacente a potenciales atacantes.
[LOW] Ruta sensible en robots.txt: Se localizó una referencia al directorio config, lo cual expone rutas privadas que no deberían ser indexadas ni visibles.