

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://21.edu.ar/  
Dominio 21.edu.ar  
Fecha 12 de mayo de 2026 a las 21:32

Checks 9 pruebas  
Hallazgos 54 totales  
Problemas 8 detectados

# B

## 83/100

puntos de seguridad

### RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 83/100 con una calificación de grado B. Durante el escaneo se ejecutaron 9 comprobaciones pasivas, de las cuales 6 fueron satisfactorias, 2 generaron advertencias y una resultó en fallo. El sistema demuestra una implementación robusta de cifrado SSL/TLS y redirecciones seguras, pero presenta debilidades críticas en las cabeceras de seguridad y exposición de puertos. En conclusión, el sitio se considera mayormente seguro, aunque es vulnerable a ataques de clickjacking y degradación de seguridad por contenido mixto.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, X-C...
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	2 cookies, todas con flags correctos
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
70 dias restantes (expira: 2026-07-21T14:47:54.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2025-07-09T15:12:51.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 55/100

Estado: FALLO

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

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

- INFO **Content-Security-Policy**  
Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**  
Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**  
Presente: max-age=31536000
- MEDIO **X-Content-Type-Options**  
Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**  
Presente: no-referrer-when-downgrade
- 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://21.edu.ar/
- INFO **HSTS (Strict-Transport-Security)**  
HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**  
HSTS no 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
- BAJO **Meta generator**  
Expone: HubSpot
- 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 — 100/100

---

Estado: OK

2 cookies, todas con flags correctos

- INFO **Cookies detectadas**  
2 cookie(s) encontrada(s)
- INFO **Cookie: \_\_cf\_bm — HttpOnly**  
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: \_\_cf\_bm — Secure**  
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: \_\_cf\_bm — SameSite**  
SameSite=none
- INFO **Cookie: \_cfuid — HttpOnly**  
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: \_cfuid — Secure**  
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: \_cfuid — SameSite**  
SameSite=none

## Contenido Mixto — 60/100

---

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**  
http://21.edu.ar?hsLang=es
- MEDIO **Recurso HTTP (href (link/stylesheet))**  
http://21.edu.ar?hsLang=es

## Robots.txt y Sitemap — 100/100

---

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**  
Presente (165 bytes)
- INFO **Reglas robots.txt**  
5 Disallow, 0 Allow
- INFO **sitemap.xml**  
Presente, 930 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 autenticación 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos o iframes, facilitando ataques de clickjacking.
- [MEDIUM] X-Content-Type-Options: No se impide que el navegador intente adivinar el tipo de contenido, lo que puede derivar en ataques de ejecución de scripts maliciosos.
- [MEDIUM] Permissions-Policy: Falta definir qué APIs del navegador pueden utilizarse, permitiendo potencialmente el acceso no restringido a la cámara o micrófono.
- [MEDIUM] Contenido Mixto: Se detectaron dos recursos cargados mediante HTTP (<http://21.edu.ar?hsLang=es>), lo que compromete la integridad del cifrado HTTPS.
- [MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, exponiendo un servidor web alternativo o proxy que amplía la superficie de ataque innecesariamente.
- [LOW] Server header expuesto: El servidor responde con la cabecera Server: cloudfare, revelando información sobre la infraestructura tecnológica utilizada.
- [LOW] Meta generator: El código fuente expone el uso de la tecnología HubSpot, lo que ayuda a recolectar información sobre el entorno de desarrollo.