# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://proveedores.eldorado.com.uy | Checks | 9 pruebas |
| Dominio | proveedores.eldorado.com.uy | Hallazgos | 58 totales |
| Fecha | 29 de julio de 2026 a las 15:53 | Problemas | 15 detectados |

**B**

75/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 75/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo. La plataforma demuestra una implementación sólida en cuanto a cifrado SSL y redirecciones seguras. Sin embargo, la ausencia de cabeceras de protección y la configuración inadecuada de cookies representan riesgos de seguridad. En su estado actual, el sitio se considera moderadamente seguro pero vulnerable a ataques dirigidos de secuestro de sesión e inyección.

## Resumen de Riesgos

| 0 | 4 | 9 | 2 | 43 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 45 dias |
| Cabeceras de Seguridad | 20 | FALLO | Solo 1/6 presentes. Faltan: Content-Security-Pol... |
| 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 | GX_CLIENT_ID: falta Secure; GX_CLIENT_ID: falta ... |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 60 | AVISO | Falta sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 8080 (HT... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-09-12T19:05:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-14T19:05:38.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: SAP — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://portalproveedoresdilz7j28e5.br1.hana.ondemand.com/portalproveedores/servlet/com.edportalprovscp.webacreedoreslogin
- 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
- BAJO **Meta generator**
  Expone: GeneXus Java 15_0_9-121631

## Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

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

## Seguridad de Cookies — 67/100

Estado: AVISO

GX_CLIENT_ID: falta Secure; GX_CLIENT_ID: falta SameSite; GX_SESSION_ID: falta Secure; GX_SESSION_ID: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: JSESSIONID — SameSite**
  SameSite=none
- INFO **Cookie: GX_CLIENT_ID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: GX_CLIENT_ID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GX_CLIENT_ID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: GX_SESSION_ID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: GX_SESSION_ID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GX_SESSION_ID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: BIGipServerportalproveedoresdilz7j28e5.br1.hana.ondemand.com — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: BIGipServerportalproveedoresdilz7j28e5.br1.hana.ondemand.com — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: BIGipServerportalproveedoresdilz7j28e5.br1.hana.ondemand.com — SameSite**
  SameSite=none

## 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 sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

## 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 ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking mediante el uso de marcos o iframes.
[HIGH] Cookie GX_CLIENT_ID (Secure): La falta del flag Secure permite que la cookie se envíe a través de conexiones HTTP no cifradas, exponiendo datos del cliente.
[HIGH] Cookie GX_SESSION_ID (Secure): La ausencia del flag Secure en la cookie de sesión permite la interceptación de credenciales en redes no protegidas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, pudiendo ejecutar archivos con contenido malicioso.
[MEDIUM] Cookie GX_CLIENT_ID (SameSite): La falta de este atributo hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie GX_SESSION_ID (SameSite): La carencia del flag SameSite en la sesión principal incrementa el riesgo de acciones no autorizadas mediante CSRF.
[MEDIUM] Referrer-Policy: No se ha definido una política para controlar qué información de referencia se envía a otros dominios al navegar.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono desde el código del sitio.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos de la infraestructura.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que representa una superficie de ataque adicional fuera del puerto estándar.
[MEDIUM] Configuración Robots.txt: El archivo bloquea el rastreo de todo el sitio, lo cual puede ser un indicativo de configuraciones que se intentan ocultar pero quedan expuestas.
[LOW] Server header expuesto: La cabecera revela el uso de tecnología SAP, facilitando a atacantes la búsqueda de vulnerabilidades específicas para ese software.
[LOW] Meta generator expuesto: El código fuente revela el uso de GeneXus Java 15_0_9-121631, exponiendo la versión exacta del entorno de desarrollo.