

# Security Headers Report

Análisis de cabeceras de seguridad HTTP

Objetivo: <https://vepiex.sial.ec/web/login>

Generado: 05/09/2026 16:21

59%

Riesgo Medio

URL analizada: <https://vepiex.sial.ec/web/login>

Seguridad

11

Analizados

4

Presentes

7

Faltantes

## Headers Presentes (4)

### HSTS (HTTP Strict Transport Security) PRESENTE

Fuerza a los navegadores a usar HTTPS exclusivamente, protegiendo contra ataques de downgrade y secuestro de cookies.

**Valor:** max-age=31536000; includeSubDomains; preload

### CSP (Content Security Policy) PRESENTE

Define qué recursos pueden cargarse en la página. Es la defensa más efectiva contra ataques XSS y de inyección de datos.

**Valor:** frame-ancestors 'self'; frame-src 'self' <https://28001.navixy.com> <https://premium.sial.ec> [https://\\*.sial.ec](https://*.sial.ec) <https://bsmart.piusi.com> <https://smartws.piusi.com>;

## X-Frame-Options **PRESENTE**

Previene ataques de clickjacking al controlar si la página puede ser embebida en iframes.

Valor: SAMEORIGIN

## X-Content-Type-Options **PRESENTE**

Evita que el navegador interprete archivos como un tipo MIME diferente al declarado (MIME sniffing).

Valor: nosniff

## Headers Faltantes (7)

### X-XSS-Protection **FALTANTE BAJO**

Activa el filtro XSS integrado en navegadores antiguos. Aunque obsoleto, proporciona protección adicional.

Recomendación: 1; mode=block

### Referrer-Policy **FALTANTE MEDIO**

Controla cuánta información del referrer se envía en las peticiones. Protege la privacidad del usuario.

Recomendación: strict-origin-when-cross-origin

### Permissions-Policy (Feature-Policy) **FALTANTE MEDIO**

Controla qué APIs del navegador puede usar la página (geolocalización, cámara, micrófono, etc.).

Recomendación: geolocation=(), microphone=(), camera=()

### X-Permitted-Cross-Domain-Policies **FALTANTE BAJO**

Controla cómo Adobe Flash y PDF pueden acceder a datos del sitio.

Recomendación: none

### COEP (Cross-Origin Embedder Policy) **FALTANTE BAJO**

Previene la carga de recursos cross-origin que no otorguen permiso explícito. Junto a COOP habilita el aislamiento de origen (cross-origin isolation).

**Recomendación:** require-corp

## **COOP (Cross-Origin Opener Policy)** **FALTANTE** BAJO

Aísla el contexto de navegación de la página de ventanas cross-origin, mitigando ataques de canal lateral (Spectre) y tabnabbing.

**Recomendación:** same-origin

## **CORP (Cross-Origin Resource Policy)** **FALTANTE** BAJO

Controla qué orígenes pueden incrustar este recurso, protegiendo frente a ataques de robo de recursos cross-origin (side-channel).

**Recomendación:** same-origin