[CIBERPLANETA]

Security Headers Report

Análisis de cabeceras de seguridad HTTP

Objetivo: `https://propeep.gob.do/`

Generado: 26/08/2026 12:27

100%

Seguridad

Riesgo Bajo

URL analizada: `https://propeep.gob.do/`

11	11	0
Analizados	Presentes	Faltantes

Headers Presentes (11)

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: `default-src 'self' https:; script-src 'self' 'nonce-kd8_uMzJ-GSpCl-AlFJvNBXa' 'unsafe-eval' https:; script-src-elem 'self' 'nonce-kd8_uMzJ-GSpCl-AlFJvNBXa' https:; require-trusted-types-for`

```
'script':; script-src-attr 'none'; style-src 'self' 'nonce-kd8_uMzJ-GSpCl-AlFJvNBXa' https:;
style-src-elem 'self' 'nonce-kd8_uMzJ-GSpCl-AlFJvNBXa' https:; style-src-attr 'unsafe-inline'; img-src
'self' https: data: blob:; font-src 'self' https: data:; connect-src 'self' https: wss:; frame-src
'self' https:; media-src 'self' https: blob:; worker-src 'self' blob:; child-src 'self' https: blob:;
object-src 'none'; frame-ancestors 'self'; base-uri 'self'; form-action 'self' https:;
upgrade-insecure-requests;
```

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

X-XSS-Protection PRESENTE

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

Valor: 1; mode=block

Referrer-Policy PRESENTE

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

Valor: strict-origin-when-cross-origin

Permissions-Policy (Feature-Policy) PRESENTE

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

Valor: camera=(), microphone=(), geolocation=(), usb=()

X-Permitted-Cross-Domain-Policies PRESENTE

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

Valor: none

COEP (Cross-Origin Embedder Policy) PRESENTE

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

Valor: `unsafe-none`

COOP (Cross-Origin Opener Policy) PRESENTE

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

Valor: `same-origin`

CORP (Cross-Origin Resource Policy) PRESENTE

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

Valor: `same-origin`