

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Content Security Policy: uma primeira política, ensaiada em modo de relatório

Segurança

CÓDIGO

RLX-AO-KB-1964

VERSÃO

v2026.10.15

PAÍS · IDIOMA

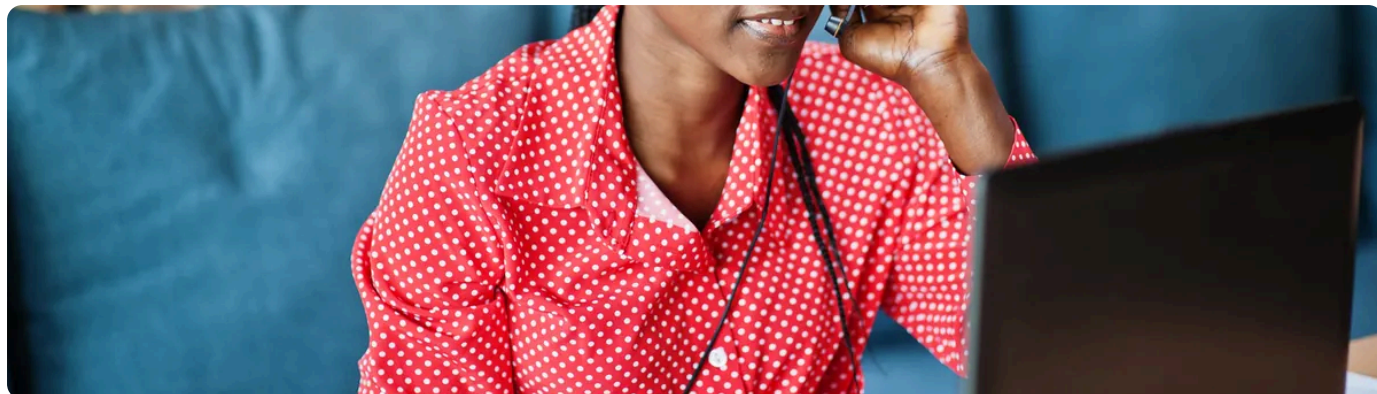
Angola · Português

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF 500 260 5724 · Matrícula 26464-25/250724

<https://www.meu.interweb.ao/knowledgebase/1964>



A resposta curta: a Content Security Policy (CSP) é um cabeçalho que diz ao navegador **de onde o site pode carregar scripts, estilos e imagens**. Se alguém injetar um script de fora, o navegador recusa-o. É forte, mas também é fácil de estragar um site com ela; por isso começa-se em **modo de relatório**, que só avisa e não bloqueia nada.

O que o site precisa

O quê	O que fazer
O que controla	Origens permitidas para scripts, estilos, imagens, tipos de letra, vídeos e ligações do site.
Modo de relatório	O cabeçalho Content-Security-Policy-Report-Only regista o que bloquearia, sem bloquear. É o modo para ensaiar.
O que costuma quebrar	Scripts e estilos escritos dentro da própria página, o Google Analytics e o Gestor de Etiquetas, tipos de letra de fora, vídeos incorporados: Gestor de Etiquetas .
Uma primeira política	Só aceitar tudo do próprio site, e acrescentar as origens de fora que o site realmente usa.
Quando passar a bloquear	Quando o registo estiver limpo durante uns dias, em todas as páginas importantes.

Como começar

1

Faça cópia do .htaccess.

2

Ponha a política em modo de relatório com uma linha simples (acrescente depois as origens de fora): `Header set Content-Security-Policy-Report-Only "default-src 'self'"`

3

Navegue no site com a consola do navegador aberta (F12, separador Consola): cada coisa que seria bloqueada aparece como aviso.

4

Acrescente as origens de fora que o site usa de propósito (analítica, tipos de letra, vídeo), uma de cada vez.

5

Quando já não aparecem avisos, troque para o cabeçalho que bloqueia (Content-Security-Policy) e volte a testar: **Cabeçalhos de segurança**.

Uma política demasiado apertada parte o site. Se passar direto ao modo que bloqueia, pode perder o menu, o formulário ou o checkout sem aviso. Teste sempre em modo de relatório, e noutro navegador. Se algo partir, volte à cópia do .htaccess.

Se o seu site mistura conteúdo http com https, resolva isso primeiro: **Conteúdo misto**. Outro cabeçalho que se liga com cuidado: **HSTS**.

Quer ajuda a ensaiar uma política para o seu site? Abra um pedido com o endereço.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Cabeçalhos de segurança explicados: o que fazem e como os acrescentar no .htaccess

HSTS explicado: forçar o https para sempre, e a armadilha de o ligar cedo demais

Conteúdo misto depois de passar a HTTPS: o cadeado que não acende

Google Tag Manager e pixels de acompanhamento: como pô-los sem tornar o site lento

ModSecurity e firewalls de aplicações web: o que fazem, e o que fazer quando um bloqueia o seu pedido



Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

Interweb Angola

RLX Angola, Lda. • Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao • +244 942 011 191 • www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado