

Protocolo de seguridad a través de "HTTPS"

En la barra de direcciones del navegador, se observa una conexión segura con el ícono en forma de candado del lado izquierdo de la dirección URL de <https://www.aescol.com/>

A través de los diferentes navegadores se puede constatar la seguridad en la conexión como se indica a continuación:

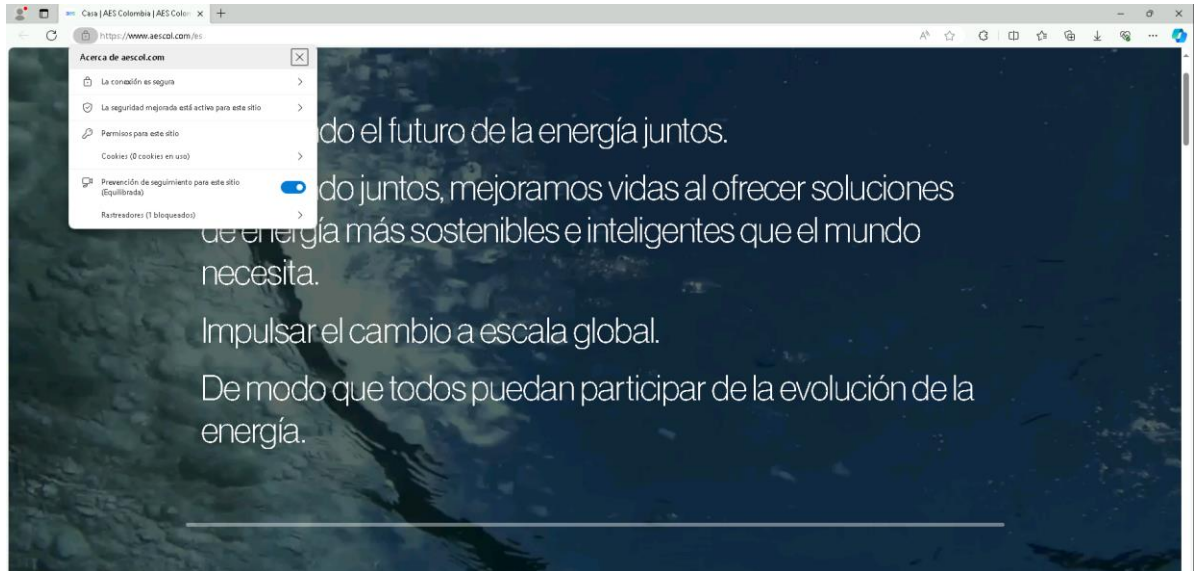
1. Firefox



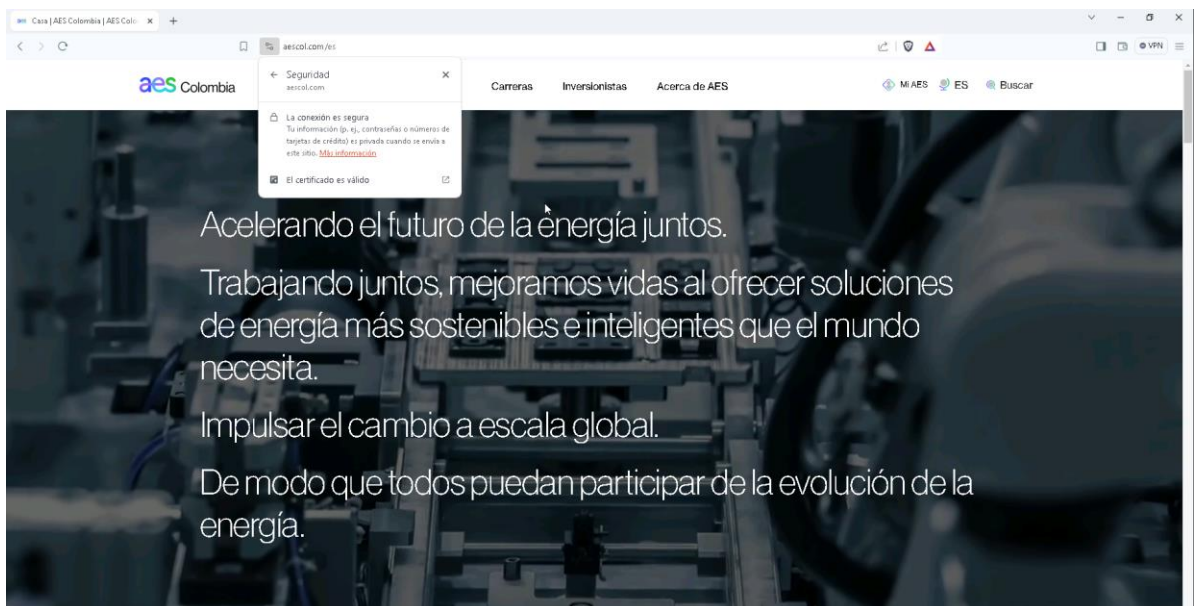
2. Google Chrome



3. Microsoft Edge



4. Brave





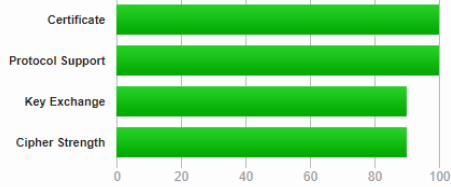
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.aescol.com](#)

SSL Report: [www.aescol.com](#) (54.160.48.22)

Assessed on: Thu, 14 Mar 2024 22:48:49 UTC | [HIDDEN](#) | [Clear cache](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	*.aescol.com Fingerprint SHA256: d054e18886672d5530845a11296c87c7eb78d764785d94e2228414333f861c95 Pin SHA256: 9gsUaUFDf4Yyi+VQ4whA6xhEULVyxXgIrYV8aqLw0=
Common names	*.aescol.com
Alternative names	*.aescol.com aescol.com
Serial Number	00a4d53905b51a50
Valid from	Mon, 03 Apr 2023 00:56:40 UTC
Valid until	Sat, 04 May 2024 00:56:40 UTC (expires in 1 month and 19 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Go Daddy Secure Certificate Authority - G2 AIA: http://certificates.godaddy.com/repository/gdig2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.godaddy.com/gdig2s1-5430.crl OCSP: http://ocsp.godaddy.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)



Certificates provided	2 (2913 bytes)
Chain issues	None
#2	
Subject	Go Daddy Secure Certificate Authority - G2 Fingerprint SHA256: 973a41276ffd01e027a2aad49e34c37846d3e076ffa820b6712e33832041aa5 Pin SHA256: 8Rw60Ej3Tt8RRkrq+WYDS9n7IS03bk5bjPUXPtaY8=
Valid until	Sat, 03 May 2031 07:00:00 UTC (expires in 7 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	Go Daddy Root Certificate Authority - G2
Signature algorithm	SHA256withRSA

Configuration



Protocols

TLS 1.3	No
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI