

DIRECCIÓN GENERAL DEL PATRIMONIO DEL ESTADO

SUBDIRECCIÓN GENERAL DE COORDINACIÓN DE LA CONTRATACIÓN ELECTRÓNICA

Instrucciones para evitar aviso de seguridad de Google Chrome

Fecha : 14/10/2015

INSTRUCCIONES PARA EVITAR AVISO DE SEGURIDAD EN GOOGLE CHROME

Posible problema

Si usted es usuario del navegador Google Chrome es posible que reciba un aviso de seguridad al acceder a la Plataforma de Contratación del Sector Público.

Es posible que su navegador le marque tachado en rojo un candado a la izquierda de la barra de direcciones en la que introduce la dirección del sitio web que está visitando, y le muestre un aviso de seguridad si pulsa sobre el mismo.

← → C	But ps://contrataciondelestado.es/wps/portal	/plataforma
Inicio	contrataciondelestado.es >> En este sitio se utiliza una configuración de seguridad >> vulnerable (firmas SHA-1), de modo que es posible que tu conexión no sea privada. >> Permisos Conexión	CITACIÓN DEL SECTOR PÚBLICO Organismos Públicos Infor
	 FNMT-RCM ha verificado la identidad de este sitio web. El servidor no ha proporcionado información de Transparencia de certificados. La cadena de certificados de este sitio web incluye al menos un certificado que se ha firmado con un algoritmo de firma obsoleto basado en SHA-1. Datos del certificado 	ontratante
Bier En la Plata La informa Además, la La platafor Los usuari NC	Cu conexión con contrataciondelestado.es está cifrada con un conjunto de cifrado obsoleto. La conexión utiliza TLS 1.2. La conexión se ha encriptado y autenticado con AES_128_GCM, y utiliza RSA como el mecanismo de intercambio clave. 2Necesitas ayuda?	ón del Sector Público n cualquier organismo del Sector Pi tratante del Sector Público puede co ratuitos y personalizados a través o ervicios que les facilitan realizar la c eder a estos servicios a través del a

El problema reportado por Google Chrome indica que el sitio utiliza firmas SHA-I, de modo que es posible que la conexión no sea privada. Puede comprobar que el sitio es seguro accediendo con otros navegadores como Internet Explorer o Mozilla Firefox, que no reportan ningún problema de seguridad.

El mensaje reportado por el navegador no es correcto. Si accede a los datos del certificado podrá ver que la Plataforma utiliza un certificado de servidor



expedido por la Fábrica Nacional de Moneda y Timbre (FNMT) con algoritmo de firma SHA-256.

rtificado General Detalles Ruta de certif	ficación		
Mostrar: <pre></pre>	•		
Campo	Valor		
📴 Versión	V3 =		
📴 Número de serie	14 e2 18 fc 18 52 9b 60 54 db 🧴		
🛅 Algoritmo de firma	sha256RSA		
🛅 Algoritmo hash de firma	sha256		
Emisor	AC Componentes Informáticos		
🛅 Válido desde	miércoles, 11 de febrero de 20		
🛅 Válido hasta	domingo, 11 de febrero de 20		
Suieto	contrataciondelsectoroublico o		



Solución

Según las indicaciones remitidas por la FNMT el problema se produce en aquellos equipos que tienen instalados certificados de "Entidades de certificación raíz de confianza" o "Entidades de certificación intermedios" de la FNMT con algoritmo de firma SHA-1.

El problema se resuelve eliminando estos certificados de sus listas de confianza siguiendo los pasos que se indican a continuación:

I. Acceda a la configuración de Google Chrome





2. Acceda a "Mostrar configuración avanzada" en la parte inferior de la pantalla

Configuración	Buscar aiustes
Iniciar sesión	L alayses
Inicia sesión para acceder a tus pestañas, tus marcadores, tu historial y tu configuración en to	odos tus dispositivos.
Además, iniciarás sesión automáticamente en tus servicios de Google. Más información	
Iniciar sesión en Chrome	
Al abrir el navegador	
Abrir la página Nueva pestaña	
 Abrir todo como estaba antes de cerrar 	
Abrir una página específica o un conjunto de páginas. Establecer páginas	
Aspecto	
Buscar temas Restablecer tema predeterminado	
Mostrar el botón Página de inicio	
Mostrar siempre la barra de marcadores	
Buscar	
Especifica el motor de búsqueda que se debe utilizar al realizar una búsqueda desde el omni	box.
Google Administrar motores de búsqueda	
Habilitar "Ok Google" para iniciar una búsqueda por voz. Más información	
Di "Ok Google" en una nueva pestaña y en google.es	
First user (actual)	
Habilitar navegación como invitado	
Deiar que cualquier nueda añadir a una nercona a Chrome.	
Dejai que cualquei pueda anadir a una persona a cinome	
Anadir persona Editar Eliminar Importar marcadores y configuración	
Navegador predeterminado	
Establecer Google Chrome como navegador predeterminado	
Google Chrome no es actualmente tu navegador predeterminado.	
Mostrar configuración avanzada	



3. Seleccione "Administrar certificados" en el área "HTTP/SSL"





4. En la lista de certificados de "Entidades de certificación intermedias" busque el certificado emitido para AC Componentes Informáticos por "AC RAIZ FNMT-RCM"

ertificados		Carling-water		×
Propósito planteado: <a> 				•
Personal Otras personas Ent	idades de c	ertificación intermedias	Entidades de ce	rtificaci 🚹 🕨
Emitido para		Emitido por	Fecha de	Nombr 🔶
AC Administración Pública AC APE AC APE AC CAMERFIRMA AAPP AC Camerfirma Certificado AC Camerfirma Express Co AC Camerfirma Express Co AC Componentes Informát AC RAIZ FNMT-RCM	os Camer orporate ticos III	AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM Chambers of Commer Chambers of Commer AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM	21/05/2022 03/11/2023 03/11/2023 20/02/2022 09/02/2034 18/01/2019 27/06/2028 01/01/2030	<ningi <ningi <ningi <ningi <ningi <ningi <ningi <ningi <ningi< td=""></ningi<></ningi </ningi </ningi </ningi </ningi </ningi </ningi </ningi
Importar Exportar Propósitos planteados del certifi <todos></todos>	Quitar		Opciones a	vanzadas Ver
Obtener más información acerca	de <u>certifica</u>	dos	C	Cerrar



5. Pulse en "Ver" y compruebe el certificado utiliza un algoritmo de firma SHA-I dentro de la pestaña "Detalles"

Certificado		
General Detalles Ruta de certif	ficación	
Mostrar: <a>(<todos>)</todos>	•	
Campo	Valor	
Versión	V3 3e 7c fd 54 cd e5 e1 6d 51 cc	=
Algoritmo de firma	sha 1RSA sha 1	
Emisor Válido desde	AC RAIZ FNMT-RCM, FNMT-R jueves, 27 de junio de 2013 1	
Válido hasta	martes, 27 de junio de 2028 1 AC Componentes Informáticos	-

6. Si efectivamente ha comprobado que este certificado utiliza el algoritmo hash de firma SHAI selecciónelo, pulse el botón quitar y acepte el mensaje de confirmación.

Certificados		1.0	Σ	×
Propósito planteado: <pre></pre>				•
Personal Otras personas Entidades de	certificación intermedias	Entidades de ce	rtificaci 1	
				Buscar ajustes
Emitido para	Emitido por	Fecha de	Nombr 🔺	· · · · · · · · · · · · · · · · · · ·
AC Administración Pública	AC RAIZ FNMT-RCM	21/05/2022	<ning< th=""><th></th></ning<>	
AC APE	AC RAIZ FNMT-RCM	03/11/2023	<ningi< th=""><th>ema de tu ordenador para conectarse a la red.</th></ningi<>	ema de tu ordenador para conectarse a la red.
AC APE	AC RAIZ FNMT-RCM	03/11/2023	<ningi< th=""><th></th></ningi<>	
AC CAMERFIRMA AAPP	Chambers of Commer	20/02/2022	<ningi< th=""><th></th></ningi<>	
AC Camerfirma Certificados Camer	Chambers of Commer	09/02/2034	<ningi< th=""><th></th></ningi<>	
AC Camerfirma Express Corporate	Chambers of Commer	18/01/2019	<ningi< th=""><th></th></ningi<>	
AC Componentes Informáticos	AC RAIZ FNMT-RCM	27/06/2028	<ningi< th=""><th>iormación</th></ningi<>	iormación
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01/01/2030	<ningi th="" 🔻<=""><th></th></ningi>	
·			•	
Importar Exportar Quita	r	Onciones a	vanzadae	n un idioma que entiendas. Administrar idiomas
		Opciones a	Valizauas	3
Propósitos planteados del certificado				
<todos></todos>				
(10005)		_		Cambiar
			Ver	
		_		arlo
Obtener más información acerca de certifica	<u>idos</u>	Certi	ficados	
			A No	No so soquirá configndo on los sortificados ornadidos nos las ontidados
Adminis	trar certificados			le certificación o cualquier otra entidad de certificación subordinada
				Desea eliminar los certificados?
Google Clo	ud Print		<u></u>	
Google clo	aarint			
Configura	r o administrar impresora	as en Go		Sí No
Adminic	trar			31 110
Adminis	crui			



7. Tras realizar este cambio vuelve a entrar en <u>https://contrataciondelestado.es</u> y compruebe que ya no se le muestra el aviso de seguridad.

