## Que es y como Instalar un Certificado Digital.

Un <u>certificado digital o certificado electrónico</u> es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido principalmente para autenticar a un usuario o sitio web en internet por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación.

El nombre asociado a esta entidad de confianza es <u>Autoridad Certificadora</u> pudiendo ser un organismo público o empresa reconocida en Internet.

El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.<sup>1</sup>

En muchas ocasiones cuando queremos acceder a una página web nos encontramos con un problema que nos indica que no podemos acceder por no disponer del certificado digital correspondiente, o en ocasiones nos sale un mensaje como el que vemos aquí:

	Esta conexión no está verificada   Ha pedido a Firefox que se conecte de forma segura a w6.seg-social.es, pero no se puede confirmar que la conexión sea segura.   Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.   ¿Qué debería hacer?   Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.		
		Detalles técnicos	
	w6.seg-social.es usa un certificado de seguridad no válido.		
	No se confía en el certificado porque el certificado emisor es desconocido.		

Donde vemos que usando el navegador de <u>Mozilla Firefox</u> nos dicen que la pagina de la Seguridad Social (w6.seg-social.es) usa un certificado de seguridad no valido y no se confía en el certificado, porque el certificado emisor es desconocido.

Este problema que con otros navegadores (Internet Explorer o Google Chrome) no pasa, se debe a los controles de seguridad que incorpora Mozilla Firefox, que no incluye entre los certificados que ya traen por defecto instalados todos los navegadores, los certificados emitidos por la FNMT (Fábrica Nacional de Moneda y Timbre), de España.

A que se debe que no se reconozca el certificado de forma correcta, pues muy simple, a que a los amigos de la FNMT les falta añadir 9 algunos datos en el certificado y por eso Mozilla Firefox presenta ese tipo de mensaje.

Si accedemos a visualizar los datos del certificado podemos ver que existen informaciones que no se han descrito por parte de la FNMT, como vemos aquí :

Visor de certi	ficados:"OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES"	×			
<u>General</u> <u>D</u> etalles					
No se pudo verificar este certificado porque el emisor es desconocido.					
Emitido para					
Nombre común (CN)	<no certificado="" de="" es="" parte="" un=""></no>				
Organización (O)	FNMT-RCM				
Unidad organizativa (OU)	) AC RAIZ FNMT-RCM				
Número de serie	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07				
Emitido por					
Nombre común (CN)	<no certificado="" de="" es="" parte="" un=""></no>				
Organización (O)	FNMT-RCM				
Unidad organizativa (OU)	) AC RAIZ FNMT-RCM				
Periodo de validez					
Comienza el	29/10/2008				
Caduca el	01/01/2030				
Huellas digitales					
Huella digital SHA-256	EB:C5:57:00:29:01:8C:4D:67:B1:AA:12:7B:AF:12:F7: 03:B4:61:1E:BC:17:B7:DA:B5:57:38:94:17:9B:93:FA				
Huella digital SHA1	EC:50:35:07:B2:15:C4:95:62:19:E2:A8:9A:5B:42:99:2C:4C:2C:20				
	Cerrar	1			

Bien.... pues este problema que en nuestro caso nos impide acceder de forma correcta a la página de la Seguridad Social y en concreto al <u>programa de cálculo de la</u> <u>pensión de jubilación</u>, lo podemos resolver de la siguiente manera.

Pulsaremos en el siguiente enlace para descargar el certificado digital de la FNMT :

https://www.sede.fnmt.gob.es/documents/11614/116099/AC\_Raiz\_FNMT-RCM\_SHA256.cer

Y seguimos los pasos que vemos en esta imagen, donde directamente se nos abre el certificado para ser instalado :







Una vez seguidos estos pasos ya tendremos incluido el certificado de la FNMT en el navegador de forma constante, para terminar lo que hay que hacer es cerrar el Mozilla Firefox y volver a iniciarlo y probar a entrar en la página de la Seguridad Social del autocalculo :

https://sede.seg-social.gob.es/Sede 1/Lanzadera/index.htm?URL=96