

gobierno De españa

MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL

# Manual de configuración de Safari en los procesos de Autenticación y Firma

Configuración del navegador de Safari para la autenticación y firma electrónica en los servicios de la Seguridad Social

Centro de Seguridad de la Información

Infraestructuras y Servicios de Seguridad

13/11/2019



Gerencia de Informática de la Seguridad Social

Versión: 1.10





# INDICE

1	Obje	tivo	. 3
2	Cuac	Iro de compatibilidad de Safari, Sistemas Operativos y tipo de firma	. 4
3	Conf	iguración del navegador	. 5
	3.1	Certificados de confianza	5
	3.1.1	Obtención del certificado raíz	. 5
	3.1.2	Instalación del certificado en los navegadores	. 5
4	Conf	iguración de Java para cada tipo de firma	. 9
	4.1	Saber la versión de Java instalada en nuestro equipo	9
	4.2	Configuración de Java en procesos de firma mediante JNLP	10
	4.2.1	Habilitar ejecutar aplicaciones de internet (Ejecutar el archivo JNLP en el proceso de firma)	10
	4.2.2	Configuración Java	11
	4.3	Configuración de Java en procesos de firma mediante Applets	12
	4.3.1	Activación del modo no seguro en Safari	12
	4.3.2	Configuración Java	14
	4.4	Configuración de Java en procesos de firma mediante Cl@ve	16
5	ANE	xos	17
	5.1	Pasos para acceder a panel de control de Java	17
	5.2	Versión del Sistema Operativo instalado	17





# 1 Objetivo

El presente documento detalla los pasos a realizar por los usuarios de cara a la configuración adecuada del navegador Safari para poder realizar operaciones de firma y/o verificación de documentos electrónicos en la Sede de la Seguridad Social.

Para saber más acerca de los sistemas de firma que utilizan los diferentes servicios web de la Seguridad Social, acuda a los manuales correspondientes.





# 2 Cuadro de compatibilidad de Safari, Sistemas Operativos y tipo de firma

(Å)	JNLP	APPLETS	CRYPTO BROWSER	CL@VE		
Windows	Θ	Θ	Θ	Θ		
Mac	Ø	${ \oslash }$	Θ	Ø		
Linux	Θ	Θ	Θ	Θ		
$\Im$ Eunciona $\bigotimes$ No funciona $\bigcirc$ No Aplica						





#### Configuración del navegador 3

#### 3.1 Certificados de confianza

Para poder validar que la conexión que se realiza a un sitio seguro, de la Seguridad Social, es válida y de confianza hay que descargarse los certificados raíces de la Seguridad Social y de la FNMT. El certificado de la Seguridad Social valida que la conexión se pueda verificar, el certificado de la FNMT garantiza que el certificado de la Seguridad Social es válido y que nadie está suplantando su identidad.

#### 3.1.1 Obtención del certificado raíz

Para descargar el certificado Raíz de la FNMT (Fábrica Nacional de Moneda y Timbre) hay que ir a la siguiente URL:

https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt,

Buscar el apartado AC Raiz FNMT-RCM y descargarlo.



#### Instalación del certificado en los navegadores 3.1.2

En la utilidad Spotlight de Mac OSX buscar la aplicación Acceso a Llaveros y pulsar en la misma.



2.- Pulsamos en la Categoría Mis Certificados para importar el mismo en dicha categoría.

0	0		Acceso a Lla	veros			
	Haga clic para blo	quear el llavero inicio de sesiór	1.		(	۹	
4	Llaveros inicio de sesión						
	Sistema						
	Certil sistema						
		Nombre	Clase	Caducidad	Llavero		_
	Categoría						
<sup>№</sup>	Todos los items Contraseñas						
	Certificados						_
	Mis certificados						
T a	Notas seguras						
1 -	-						
							_
		+ i		0 ítems			
-							

3.- Vamos al menú de la barra superior y desplegamos la opción **Archivo**. Elegimos **Importar** elementos....

Nuevo ítem de contraseña Nuevo ítem de nota segura Nuevo llavero	第N 公第N て第N				
Importar elementos Exportar elementos	<mark> </mark>				
Añadir llavero Eliminar el llavero "inicio de sesión"	☆第A て第≪				
Cerrar	жw				
Obtener información	жI				
Bloquear llavero "inicio de sesión" Bloquear todos los llaveros	ЖL				
Convertir el llavero "inicio de sesión" en el llavero por omis					

4.- Nos aparecerá una ventana de diálogo en la que buscaremos el certificado que queremos importar, lo resaltamos y pulsamos en **Abrir**.



6.- Veremos cómo se ha importado correctamente el mismo. Si el certificado está caducado también se informará de lo mismo y será necesario renovarlo para que sea funcional.

00	0			Acceso a Ll	averos		
Haga clic para bloquear el llavero inicio de sesión.					٩		
L ini Mi Sis Ce	Llaveros Inicio de sesión Micrertificates Sistema Certificate Sistema Certificates Sistema Certificates Sistema Certificates Sistema Certificates Sistema Certificates Sistema						
		Nombre	A	Clase	Caducidad	Llavero	
		NOMBRE	Indexter CRUP Centures	certificado	16/02/2010 0:	inicio de sesión	
Ca	ategoría						
泳 To	odos los ítems						
📴 Ce	ertificados						
🖾 Mi	is certificados						
	aves otas seguras						
	-						
		+ i			1 ítem		

7.- Podemos cerrar la aplicación Acceso a Llaveros accediendo al menú superior y pulsando **Salir de Acceso a Llaveros**. Ya podremos acceder a direcciones dónde se solicite el certificado digital que acabamos de instalar.





Acceso a Llaveros	Archivo	Edición				
Acerca de Acceso	a Llaveros	5				
Preferencias	Preferencias					
Primera Ayuda de Asistente para Cer Visor de tickets Ke	Llavero tificados erberos	C第A ▶ べひ第K				
Servicios		•				
Ocultar Acceso a L Ocultar otros Mostrar todo	laveros.	田光 日第フ				
Salir de Acceso a L	laveros	жo				





## 4 Configuración de Java para cada tipo de firma

#### 4.1 Saber la versión de Java instalada en nuestro equipo

Acceda al panel de control de Java (ver anexo: Acceder al panel de control de Java)

En el "Panel de control de Java" seleccionar la pestaña Java y después pulsar el botón "Ver..." se abrirá otra pantalla.



En la pantalla que se muestra un listado con las instalaciones de Java que tiene el equipo. En la columna "Producto", se puede ver la versión instalada.

Se recomienda disponer de una única instalación de Java actualizada. Si dispusiera de más de una máquina virtual de Java instalada, acceda al panel de control del Sistema Operativo y desinstale las versiones más antiguas.





#### 4.2 Configuración de Java en procesos de firma mediante JNLP

Cuando se proceda a la firma JNLP, ejecutar el archivo descargado en Safari con "Java Web Start"

#### 4.2.1 Habilitar ejecutar aplicaciones de internet (Ejecutar el archivo JNLP en el proceso de firma)

Para que Mac permita ejecutar aplicaciones descargadas de internet (Ejecutar el archivo JNLP en el proceso de firma)

#### • En versiones Mac anteriores a Sierra (Yosemite, Capitán)

Hay que entrar:

Preferencias del Sistema > Seguridad y Privacidad. Debemos estar dentro de la pestaña General y ver que abajo del todo aparezca Permitir aplicaciones descargadas de Cualquier sitio

(Si las opciones están bloqueadas hay que pulsar el icono del candado)

#### • En versión Mac sierra:

Lo primero será abrir la app de Terminal. Para eso puedes ir a Aplicaciones y escribe terminal para buscar esta aplicación.

Una vez abierta debes escribir el siguiente comando: sudo spctl --master-disable

Te pedirá la contraseña de administrador, Admin, para confirmar los cambios.

Ahora regresamos a Preferencias del Sistema > Seguridad y Privacidad. Debemos estar dentro de la pestaña General y ver que abajo del todo aparezca Permitir aplicaciones descargadas de Cualquier sitio. Igual que la captura que tienes a continuación

Si quisieras volver a la configuración inicial solo tienes que volver a abrir Terminal y escribir el siguiente comando:

sudo spctl --master-enable





#### 4.2.2 Configuración Java

Acceda al panel de control de Java (ver anexo: Acceder al panel de control de Java)

Una vez dentro, acceder a la pestaña "Avanzado"

• Para la primera vez que se ejecuta el proceso de firma se recomienda no activar la opción: "No solicitar la selección de certificados de cliente cuando no exista ningún certificado o exista sólo uno"

🌆 Pane	l de Co	ontrol de Ja	va			_		$\times$
General	Java	Seguridad	Avanzado					
Verifica	No solicitar la selección de certificados de cliente cuando no exista ningún certificado o exista     Nostrar el certificado del sitio no se corresponde con el nombre del host     Mostrar el certificado del sitio desde el servidor incluso si es válido     Verificación de seguridad de código mixto (sandbox frente a de confianza)     Activar: mostrar advertencia si es preciso     Activar: ocultar advertencia y ejecutar con protecciones     Activar: ocultar advertencia y no ejecutar código que no sea de confianza     Desactivar verificación (no recomendado)							
Compro	Certific Todos No com bar rev	ado de publi los certificad nprobar (no r vocación de e	cador sólo os en la cad recomendado certificado d	ena de confianza )) e código firmado con	-			
	Listas ( Online	de Revocació Certificate S	ones de Cert	ficados (CRL)	-			

Si estuviera habilitado no se mostraría la ventana de elección de certificado en el momento de la identificación; al menos en esta primera vez es necesario que esta opción se desmarque.

Tras esta primera ejecución, se puede dejar activada, de este modo se evitaría mostrar la selección del certificado en este punto, ahorrando un paso en el proceso.

• Activar la opción "Usar los certificados y claves del almacén de claves del explorador"

🔬 Panel de Control de Java — 🗌 🔿							
General Java Seguridad Avanzado							
Realizar comprobaciones de revocación de certificado TLS en Certificado de servidor solo Todos los certificados en la cadena de confianza No comprobar (no recomendado) Comprobar revocación de certificado TLS con Listas de Revocaciones de Certificados (CRL) Online Certificate Status Protocol (OCSP) CCL y OCSP Valores de Senuridad Avanzada							
Activar el entorno restringido del sistema operativo (sandbox nativo) Ulsar los certificados y daves del almacén de claves del explorador Activar comprobación de revocación de la lista negra Activar almacenamiento en caché de contraseña para autenticación Acteptar Cancelar Aplicar							



SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL



#### **¡IMPORTANTE!**

El proceso de firma debe realizarse en menos de cinco minutos, la demora puede dar lugar a un error al finalizar el proceso de firma

#### 4.3 Configuración de Java en procesos de firma mediante Applets

#### 4.3.1 Activación del modo no seguro en Safari

Es necesario activar el modo no seguro en las páginas de la sede electrónica para que el navegador pueda acceder a los archivos locales del equipo y ejecutar el proceso de firma electrónica de forma satisfactoria.

Acceder a la sede electrónica en Safari: https://sede.seg-social.gob.es



#### Ir a preferencias de SAFARI

->pestaña seguridad/security

->Ajustes de módulo/pug-in setting





Poner en modo no seguro los sitios web que aparezcan de la sede electrónica de la seguridad social con "ejecutar modo no seguro"

Permitir WebGL

Módulos de Internet: 🗹 Permitir módulos

Bloquear ventanas emergentes

Ajustes de WebGL...

Ajustes de módulo.

?

- w2.seg-social.es
- w6.seg-social.es
- sede.seg-social.gob.es

(Puede que no aparezcan las 3)

000	Seguridad	V
General Pestañas Autorrelleno Contraso	Privacidad Notificaciones	Extensiones Avanzado
Java Versión Java 8 Update 131	Java Permitir que los sitios web utilicen este módul	o con los aiustes siguientes:
	Sitios web configurados	Preguntar
	🚱 w2.seg-social.es	✓ Activado
	📀 safari-extensions.apple.com 🗸 Activar la protecció	
	— Al visitar otros sitios	web: Activado

#### (ATENCION)

Si la opción "ejecutar modo no seguro" no aparece hay que mantener pulsado el botón "option key" del teclado y la opción aparecerá.

(Esta opción estará oculta en las versiones más recientes de Safari)



Una vez puesto el modo no seguro en las direcciones de la sede electrónica, se podrá firmar con normalidad.

#### 4.3.2 Configuración Java

Acceda al panel de control de Java (ver anexo: Acceder al panel de control de Java)

Una vez en "Panel de control de Java" pulse en editar lista de sitios (Véase imagen)



Pulse en agregar y añada las siguientes direcciones web:

- https://w2.seg-social.es
- https://w6.seg-social.es
- https://w7.seg-social.es





🔬 Lista de excepciones de sitios	×
Las aplicaciones iniciadas desde los sitios que se enumeran a continuación se podrán ejecutar después de las peticiones de datos de seguridad apropiadas.	:
Ubicación	]
https://w2.seg-social.es	
https://w6.seg-social.es	
https://w7.seg-social.es	
Agregar Eliminar Eliminar	]
Se recomienda el uso de sitios HTTPS si están disponibles.	
Aceptar Cancelar	

Pulse "Aceptar" y vuelva a la pestaña de seguridad. Marque las siguientes opciones:

- Activar el contenido java en el explorador
- Nivel de seguridad alta
- Restaurar peticiones de Datos de seguridad

🛃 Panel de Control de Java	_		×						
General Actualizar Java Seguridad Avanzado									
Activar el contenido Java en el explorador									
Nivel de seguridad de las aplicaciones que no están en la lista de excepción de sitios O Muy Alta									
de certificación de confianza y solo si el certificado se puede verificar como no revocado.									
certificado. Lista de excepciones de sitios Las aplicaciones iniciadas desde los sitios que se enumeran a continuación se podrán ejecutar después de las peticiones de datos de seguridad apropiadas. http://badaral.map.es https://www.registradores.org/									
Restaurar Peticiones de Datos de Seguridad Gestionar Certificados									
Aceptar	Cancelar	Apli	icar						





#### Acceda la pestaña General

Botón: "Configuración" -> Botón: "suprimir archivos" -> Marcar las 3 opciones y aceptar.

🛃 Panel de Control de Java	– 🗆 X
General Actualizar Java Seguridad Avanzado	
Acerca de	
Consulte la información sobre la versión del panel de control de Java.	
	Acerca de
Configuración de Red	
La configuración de red se utiliza cuando se establece la conexión a Internet defecto la configuración de red del explorador web. Esta configuración sólo usuarios con conocimientos avanzados.	:. Java utilizará por debe ser modificada por
Co	onfiguración de Red
Archivos Temporales de Internet	
Los archivos utilizados en las aplicaciones de Java se guardan en una carpet su ejecución posterior. Sólo los usuarios con conocimientos avanzados deber modificar esta configuración.	a especial para acelerar rían suprimir archivos o
Configuración	Ver
El explorador tiene Java activado.	-
Configuración de Archivos Temporales	~
configuración de Archivos temporares	^
Conservar Archivos Temporales en mi Computadora	
Ubicación	
Seleccione la ubicación en donde se guardan los archivos temporales	
C:\Users\99GU6967\AppData\LocalLow\Sun\Java\Deployment\cach	e Cambiar
Espacio en Disco	
Seleccione el nivel de compresión de los archivos JAR: Ning	guna 🗸
Establezca la cantidad de espacio en disco para el almacenamiento de	e archivos temporales:
	32768 🔶 MB
Suprimir Archivos	32768 MB

## 4.4 Configuración de Java en procesos de firma mediante Cl@ve

Si accede a un servicio con usuario y contraseña, realizará la firma mediante Cl@ve

Este tipo de firma no requiere ninguna configuración en Java





# 5 ANEXOS

## 5.1 Pasos para acceder a panel de control de Java

## > Mac/OS

Los pasos a seguir para abrir el panel de control son:

- 1. Haga clic en el icono de Apple en la esquina superior izquierda de la pantalla
- 2. Abrir preferencias del Sistema.
- 3. Abrir el icono Preferencias de Java.

## 5.2 Versión del Sistema Operativo instalado

#### > En sistemas Mac/OS

Dirigirse a la barra de tareas, hacer clic en la manzana de Apple, pulsar "acerca de este Mac"

Se mostrará la versión.