GUÍA RÁPIDA DE INCIDENCIAS EN LA FIRMA ELECTRÓNICA

INTRODUCCIÓN

Este documento pretende dar solución, de una manera concisa, a las incidencias que se presentan a la hora de realizar una firma electrónica en la aplicación Coopera 2020 y que puede llevar a la imposibilidad de realizar la misma.

No pretende ser una guía exahustiva de todas las incidencias que pueden surgir, sino más bien una fuente de consulta para las más comunes, que por otro lado son el porcentaje más significativo, así como facilitar la comprobación y configuración correcta de los programas afectados para la realización de aquella.

Se parte de la base de que se conocen los conceptos básicos relativos a la identificación, autenticación y firma electrónica (al respecto, se puede consultar información en el Portal de la Administración Electrónica <u>http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html</u>), así como estar en posesión en España de un certificado digital compatible con la plataforma @firma, o en el caso de Portugal, de la tarjeta ciudadana (cartao portuguesa). A partir del 8 de abril de 2021, para usuarios portugueses también es posible utilizar la Chave Móvel Digita (CMD) como sistema de identificación electronica para acceder a Coopera 2020. No obstante, este sistema no podrá utilizarse para firmar electrónicamente, debiendose utilizar en este caso la cartao.

sta guía se centra en la casuística derivada de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT) por ser los de uso más común, por lo que los usuarios que utilicen otros certificados digitales tendrán que realizar la interpretación analógica oportuna para determinar qué es aplicable en su caso (módulo criptográfico, instalación del certificado raíz de la entidad emisora...). A tales efectos, se recomienda acudir al sitio web del Prestador de Servicios de Certificación (PSC) que haya emitido su certificado.

El ordenador donde se ejecute la aplicación deberá reunir una serie de especificaciones (programas instalados, configuración de los mismos, lector de tarjetas inteligentes en su caso, etc.), bajo las cuales está garantizado el funcionamiento de la aplicación sin ningún tipo de problema. Se podría denominar el escenario óptimo de ejecución.

En Coopera 2020 se utiliza AutoFirma (autofirm@) en todos sus escenarios.

INSTALACIÓN DE AUTOFIRM@

Instalación de "AutoFirma"

Se puede realizar la descarga del ejecutable AutoFirma desde el Portal de Administración Electrónica, eligiendo la opción: http://firmaelectronica.gob.es/Home/Descargas.html Al descomprimir el archivo,

encontrará al menos un fichero ejecutable, que es el que debe instalar, y un documento denominado "AF_manual_instalacion_usuarios_ES.PDF", que contiene toda la información relativa a la instalación de este software. Se debe instalar en el equipo, confirmando todo lo que el asistente proporcione por defecto. Si se instala el navegador posteriormente a la instalación de Autofirma o bien se realizan actualizaciones de dicho navegador y se aprecia que el proceso de AutoFirma está dando problemas, se recomienda proceder de nuevo a la instalación de AutoFirma a través del ejecutable descargado del Portal de Administración Electrónica y el problema quedará solucionado. Se recomienda realizar la instalación de la aplicación AutoFirma con los navegadores cerrados.

ÚLTIMOS CAMBIOS

A continuación, se detalla cómo comprobar o modificar configuraciones relativas a la aplicación Coopera 2020, aunque no tengan relación directa con el proceso de firma electrónica pero sí con el correcto funcionamiento de la citada aplicación.

NAVEGADOR: INTERNET EXPLORER

Javascript activado

La activación de javascript se ha detallado en el apartado *'Escenario óptimo'* al especificar la configuración del navegador para las distintas zonas de Seguridad del mismo. Es el parámetro *'Active scripting'*, dentro de la lista de configuración del *'Nivel personalizado...'*.

Cookies activadas

Las cookies, en Internet Explorer 11, las administra automáticamente el navegador. Para asegurarse de no tener problemas con ellas, hay que acceder a las *Opciones de Internet* desde el navegador y seleccionar la pestaña *'Privacidad'*, pulsar el botón *'Sitios'* y, en la ventana emergente, añadir la dirección URL del sitio de la aplicación. En su primer tramo como se ha explicado en el inicio del apartado Incidencias de esta guía, en la caja de texto *'Dirección del sitio web:'*, se pulsa el botón *'Permitir'*. De esta manera se estará permitiendo explícitamente las cookies del sitio web de la aplicación.

	Opciones	de Inte	ernet	B	?	×		
Conexiones	Program	as	Opcie	ones avan	zadas			
General	Seguridad	Priv	acidad	Cor	ntenido			
Configuración								
 Bloquea cookies de terceros que no tienen una directiva de privacidad sólida Bloquea cookies de terceros que guardan información de contacto que se puede usar sin su consentimiento explícito Restringe cookies de origen que guardan información de contacto que se puede usar sin su consentimiento explícito 								
Sitios	Importar	Av	anzada	Predete	rminada	а		
Ubicación ——								
Nunca permitir su ubicación fís	que los sitios web so sica	liciten		Borra	r sitios			
Bloqueador de ele	mentos emergentes							
🗌 Activar el bloqu	ueador de elementos	emergen	tes	Config	uración			
InPrivate								
 Deshabilitar ba exploración de 	rras de herramientas InPrivate	y extens	iones cuand	o se inicie	la			
	Acciones de pri	vacida	d por siti	0	¢	×		
Administrar sitios								
Puede esp usar cookie	ecificar los sitios web es, independientemer	a los que ite de la d	siempre o ni irectiva de p	unca se le rivacidad	s permit que use	te en.		
Escriba la dirección exacta del sitio web que desea administrar, y después haga clic en Permitir o en Bloquear.								
Para quitar un sitio de la lista de sitios administrados, seleccione el nombre de dicho sitio web y haga clic en el botón Quitar.								
Dirección del sitio	web:							
http://azorin.centr	al.sepg.minhac.age			Ble	oquear			

 Sitios web administrados:

 Dominio
 Configuración

 Quitar todos

 En la lista 'Sitios web administrados' aparecerá el dominio del sitio web con la configuración de 'Permitir

Permitir

En la lista 'Sitios web administrados' aparecera el dominio del sitio web con la configuración de 'Permitir siempre'.

El nivel de configuración para la zona de Internet en la pestaña de *'Privacidad'* se recomienda que esté en *'Media'*.

Pop-ups (ventanas emergentes) activadas

En la ventana anterior de *'Privacidad'*, se encuentra la activación o desactivación de las ventanas emergentes, dentro del apartado *'Bloqueador de elementos emergentes'*. Tiene que estar como se muestra en la imagen siguiente (permite las ventanas emergentes).

Sitios Importar Avanzada	Predeterminada					
Ubicación						
Nunca permitir que los sitios web soliciten su ubicación física Borrar sitios						
Bloqueador de elementos emergentes						
Activar el bloqueador de elementos emergentes Configuración						
InPrivate						
Deshabilitar barras de berramientas y extensiones cuar	ndo se inicie la					

Habilitar descarga de archivos y fuentes

Se encuentra en la configuración de las zonas de seguridad del navegador ('Internet', 'Intranet local', 'Sitios de confianza') que ya se ha comentado en reiteradas ocasiones a lo largo de esta guía. Se pulsa en el botón 'Nivel personalizado...' y buscando en el grupo 'Descargas', los apartados 'Descarga de ficheros' y 'Descarga de fuentes' deben estar con el valor 'Habilitar'.



NAVEGADOR: CHROME

Javascript activado

La activación de javascript se realiza en "personaliza y controla Google Chrome" (Tres puntos verticales). En "configuración", se selecciona "Privacidad y seguridad", en esta opción, se selecciona "Configuración de sitios web" y dentro de esta opción debe de estar "**JAVASCRIPT" permitido**.

Cookies activadas

Esta opción se encuentra en "personaliza y controla Google CHROME "(Tres puntos verticales). En "configuración", se selecciona "Privacidad y seguridad", en esta opción, se selecciona "Configuración de sitios web" y dentro de esta opción debe de estar en "**Cookies y otros datos de sitios**" **como se muestra en pantalla.**

Configuración	Q, Buscar ajustes			
🛓 Google y tú	← Cookies y otros datos de sitios ② Q Buscar			
autocompletar				
Ocomprobación de seguridad				
Privacidad y seguridad				
Aspecto				
Q Buscador				
Navegador predeterminado				
() Al abrir				
Configuración avanzada 👻	Configuración general			
Extensions [2]	O Permitir todas las cookies ~			
Extensiones	Bloquear cookies de terceros en el modo de incógnito			
	 Los sitios web pueden usar cookies para mejorar tu experiencia de navegación, por ejemplo, para mantener tu sesión iniciada o recordar los artículos de tu carrito de la compra Mientras estás en modo de incógnito, los sitios web no pueden usar tus cookies para ver tu actividad de navegación en otros sitios web con el objetivo de, por ejemplo, personalizar tus anuncios. Es posible que algunos sitios no funcionen correctamente. 			
	O Bloquear cookies de terceros ~			
	O Bloquear todas las cookies (no recomendado) 🗸			
	Borrar las cookies y los datos de sitios web al salir de Chrome			
	Enviar una solicitud de no seguimiento con tu tráfico de navegación			

Pop-ups (ventanas emergentes) activadas

Esta opción se encuentra en "Personaliza y controla Google Chrome" (Tres puntos verticales). En "configuración", se selecciona "Privacidad y seguridad", en esta opción, se selecciona "Configuración de sitios web" y dentro de esta opción debe de estar en "Ventanas emergentes y redireccionados" como se muestra en pantalla (Desactivado).

Configuración Q Buscar ajustes			
•	Google y tú	Ventanas emergentes y redirecciones Q Buscar	
Ê	Autocompletar		
۲	Comprobación de seguridad	Bloqueado (recomendado)	
•	Privacidad y seguridad	Bloquear	Añadir
۲	Aspecto		
Q	Buscador	No se na anadido ningun sitio web	
	Navegador predeterminado	Permitir	Añadir

6

Habilitar descarga de archivos y fuentes

Esta opción se encuentra en "Personaliza y controla Google Chrome" (Tres puntos verticales). En "configuración", se selecciona "Privacidad y seguridad", en esta opción, se selecciona "Seguridad" y dentro de esta opción debe de estar marcada "**Protección estándar**" marcada, como se muestra en pantalla.

Con	iguración	۹	Busca	ar ajustes
÷	Google y tú	L		
Ê	Autocompletar			
۲	Comprobación de seguridad			
•	Privacidad y seguridad	Nave	egació	Śn Segura
۲	Aspecto	~	Prot	tección mejorada
Q	Buscador	0	Prot advi	tección más rápida y proactiva frente a descargas, extensiones y sitios web peligrosos. Te ierte sobre robos de contraseñas. Necesita enviar datos de navegación a Google.
	Navegador predeterminado		0	Predice y te advierte de eventos pelígrosos antes de que se produzcan
Ċ	Al abrir		G	Te protege en Chrome y puede usarse para mejorar tu seguridad en otras aplicaciones de Google
Confi	guración avanzada 🔺		•	cuando has iniciado sesión
	Idiomas		G	wejora tu segunuau y ra de todos los usuarios en la web
<u>+</u>	Descargas		07	Te avisa si tus contraseñas se ven expuestas en una quiebra de seguridad de datos
ē	Imprimir		ıl.	Envia URL a Navegación Segura para que las compruebe. También envia una muestra pequeña de páginas, descargas, actividad de las extensiones e información del sistema para contribuir a
Ť	Accesibilidad			detectar nuevas amenazas. Cuando inicias sesión, vincula estos datos a tu cuenta de Google de forma temporal para protegerte en las aplicaciones de Google.
э,	Sistema		Drot	tanaión anténdar
Ð	Recuperar ajustes y borrar	۲	Prot	lección estándar frente a descargas, extensiones y sitios web que son peligrosos.
Exten	siones 🖸		0	Detecta y te advierte de los eventos peligrosos cuando suceden
Inform	nación de Chrome		њ	Comprueba las URL guardadas en Chrome con una lista de sitios web que no son seguros. Si un sitio web intenta robarte la contraseña o te descargas un archivo dañino, puede que Chrome también envie URL, así como fragmentos de contenido de la página, a Navegación Segura.

ESCENARIO ÓPTIMO

Los programas que inciden directamente en la firma electrónica, establecidos por la División de Explotación (DIVE) de la Oficina de Informática Presupuestaria (OIP) de la Intervención General de la Administración del Estado (IGAE) para los entornos integrados de la Administración Presupuestaria (AP), son los que se indican:

SISTEMA OPERATIVO: A partir de Windows 8.1

NAVEGADOR: CHROME, Internet Explorer.

CLIENTE FNMT: Configurador FNMT. Versión 3.5 ó superior (opcional).

NOTA: Si se instala el Módulo Criptográfico, no hace falta este cliente por estar incuido en aquel.

MÓDULO CRIPTOGRÁFICO (*): TC-FNMT, versión 5.3.0 ó superior

(*) – Este software solo hace falta si el certificado digital se encuentra en una tarjeta criptográfica.

NOTA: No hace falta instalar ningún cliente para usar el DNIe ya que Microsoft lo incorpora por defecto en Windows 10

CERTIFICADO DIGITAL COMPATIBLE. Es la pieza más relevante en el proceso de firma electrónica.

Como antes se ha indicado, para certificados emitidos por otros PSC el software a instalar será el que en cada caso corresponda.

Para comprobar que los programas instalados son de las versiones correctas se puede proceder como sigue:

• SISTEMA OPERATIVO (S.O.)

Se pulsa con el botón derecho del ratón en el icono del escritorio '*Este equipo*' y se selecciona '*Propiedades*'. En la ventana emergente se pueden comprobar los datos del S.O.

Ver información básica	acerca del equipo	
Edición de Windows		
Windows 10 Enterprise © 2018 Microsoft Corporat	ion. Todos los derechos reservados.	Windows10
Procesador:	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 3.60 GHz	
Memoria instalada (RAM):	16,0 GB (15,9 GB utilizable)	
Tipo de sistema:	Sistema operativo de 64 bits, procesador x64	
Lápiz y entrada táctil:	La entrada táctil o manuscrita no está disponible para esta pantalla	

CLIENTE FNMT (opcional)

En la localización anterior (*Programas y características*), se busca la línea '*Configurador_FNMT*'. En la columna '*Versión*' se localiza la versión del programa que está instalado. Recordar que no es necesario este software si se tiene instalado el Módulo Criptográfico al estar incluido en este. En caso de necesitar instalarlo hay que visitar la web <u>www.fnmt.es</u> de la FNMT.

Desinstalar o cambiar un programa							
Para desinstalar un programa, selecciónelo en la lista y después haga clic en Desinstalar, Cambiar o Reparar.							
Organizar 🝷 Desinstalar							
Nombre	Editor	Se instaló el	Tamaño	Versión			
Sisco AnyConnect Secure Mobility Client Cisco Systems, Inc. 14/11/2018 5,85 MB 4.4.03034							
🔂 Configurador_FNMT	FNMT-RCM	12/07/2019	4,49 MB	3.7			
A 5 10 15 1	DL L C D C	05/07/2010	1.50.00	15 3 1003			

• MÓDULO CRIPTOGRÁFICO

En el mismo lugar se busca la línea 'Instalable TC-FNMT'.

Desinstalar o cambiar un programa Para desinstalar un programa, selecciónelo en la lista y después haga clic en Desinstalar, Cambiar o Reparar.							
Organizar 🕶 Desinstalar Cambiar Reparar							
Nombre	Editor	Se instaló el	Tamaño	Versión			
Marine 3 IGAE 14/11/2018 20,0 KB 1.6.1							
🕺 Instalable TC-FNMT	N Instalable TC-FNMT FNMT-RCM 30/11/2018 26,0 MB 7.0.1						
I iReport 5.6.0	laspersoft Corp.	17/05/2019		5.6.0			

Si se utiliza una tarjeta inteligente que contenga el certificado digital o el DNIe, hace falta que el ordenador disponga de un lector de tarjetas criptográficas (inteligentes) y que esté correctamente instalado. La manera rápida de verificar si está instalado el mencionado lector es accediendo al *Panel de Control - Administrador de Dispositivos* y comprobando que existe un apartado de *'Lectores de tarjetas inteligentes'* parecido al siguiente:



Además de tener instalados los programas anteriores con sus respectivas versiones es importante la configuración correcta de los mismos, ya que una configuración errónea puede causar que no se ejecute el software (AUTOFIRMA) correspondiente en el proceso de firma electrónica.

Una configuración relevante es la del navegador de Internet (Internet Explorer), que tiene que tener habilitados los complementos de Java (Plug-In) y javascript en la zona correspondiente de seguridad.

Para verificar estos puntos se necesita abrir el navegador Internet Explorer. Para comprobar que los Plugin de Java están habilitados se pulsa en la *rueda dentada*, que ya se ha utilizado para verificar la versión del mismo, y se selcciona 'Administrar complementos', buscando el grupo 'Oracle America, Inc.'. Las dos lineas que comprende este grupo tienen que tener 'Habilitado' la columna 'Estado'.

	A		
Nombre	Editor	Estado	Arquite
Adobe Systems, Incorporated			
Adobe Acrobat Create PDF Toolbar	Adobe Systems, Incorpo	Deshabilita	32 bits y
Adobe Acrobat Create PDF Helper	Adobe Systems, Incorpo	Habilitado	32 bits y
Adobe Acrobat Create PDF from Selection	Adobe Systems, Incorpo	Habilitado	32 bits y
Microsoft Corporation			
Groove GFS Browser Helper	Microsoft Corporation	Deshabilita	32 bits
Office Document Cache Handler	Microsoft Corporation	Deshabilita	32 bits y
Microsoft Windows Third Party Application Comp	oonent		
Shockwave Flash Object	Microsoft Windows Thir	Habilitado	32 bits y
No disponible			
Edit with Altova XMLSpy	No disponible	Habilitado	32 bits
Enviar a OneNote	No disponible	Habilitado	32 bits y
Notas vinculadas de OneNote	No disponible	Habilitado	32 bits y
Oracle America, Inc.			
Java(tm) Plug-In SSV Helper	Oracle America, Inc.	Habilitado	32 bits y
Java(tm) Plug-In 2 SSV Helper	Oracle America, Inc.	Habilitado	32 bits y

Para comprobar que se pueden ejecutar el código javascript, se pulsa la *rueda dentada* y se selecciona *Opciones de Internet*', y en la pestaña *'Seguridad'* se selecciona la zona en la que se quieren comprobar estos valores.



Puede ser 'Internet', 'Intranet local' o 'Sitios de confianza', se pulsa en el botón 'Nivel personalizado...' y se busca el grupo de valores 'Automatización'. Una vez localizado en la lista emergente, se comprueba que los items 'Active scripting' esté con el valor 'Habilitar'.

Configuración de seguridad: zona de sitios de confia

Configuración	
🎎 Inicio de	e sesión
	o de sesión anónimo
🗌 🗌 Inici	o de sesión automático con el nombre de usuario y
Inici	o de sesión automático solo en la zona Intranet
O Preg	guntar por el nombre de usuario y la contraseña
S Automatizad	ción
S Active s	cripting
O Des	habilitar
Habi	ilitar
() Preg	guntar
S Automat	tización de los applets de Java
() Desi	habilitar
Hab	litar
	juntar Alta XCC
	nitro XSS
<	
*Se aplicará cuan	do reinicie el equipo
Restablecer config	uración personal
Restablecer a:	Medio (predeterminado) V Restable

La ventana anterior es sustituida por la siguiente

Configuración de seguridad: zona de sitios de confianza

Configuración						
Autenticació Autenticació Inicio de Inicio Inicio Inicio Prese Autenticació Inicio Prese Inicio Ini	ón del usuario e sesión io de sesión anónimo io de sesión automático con el nombre de usuario y io de sesión automático solo en la zona Intranet guntar por el nombre de usuario y la contraseña	α				
Automatiza Active s Des Hab Preg Automa Des Hab Preg Habilitar	Automatización Active scripting Deshabilitar Preguntar Automatización de los applets de Java Deshabilitar Habilitar Preguntar Preguntar					
<	2					
*Se aplicará cuar	ndo reinicie el equipo					
-Restablecer config	guración personal					
Restablecer a:	Medio (predeterminado) ~ Restablece	er				
	Aceptar Can	celar				

 \times

Esta operación se puede realizar en las 3 zonas o como se verá en el apartado de Incidencias, solo en la zona de 'Sitios de confianza'.

INICIDENCIAS

Con carácter general, si en el transcurso del proceso de firma se produce algún error o incidencia que hiciera que no se terminase el proceso, hay que **cerrar completamente el navegador** y reiniciar la operación.

Es altamente recomendable añadir el sitio desde donde se ejecuta la aplicación (URL), poniendo solamente el primer tramo de la misma (por ejemplo: <u>https://webpub2.igae.hacienda.gob.es</u>) en los Sitios de confianza del navegador para evitar los bloqueos.

En INTERNET EXPLORER:

Esto se consigue en '*Panel de control - Opciones de Internet*', en la pestaña de '*Seguridad*', eligiendo la zona 'Sitios de confianza':

6		Propiedad	des: Inte	ernet	¢	?	х
Con	exiones	Program	as	Орс	iones avanz	zadas	
Gene	ral	Seguridad	Priv	acidad	Contenido		
Seleccion	ne una zona pa	ara ver o cambia	r la config	uración de	seguridad.		,
	🥥 🔩 🗸 🚫						
Int	ternet	Intranet local	Sitios de	confianza	Sitios restri	ngidos	
	Sitios de co Esta zona con van a perjudio	nfianza ntiene sitios web car a su equipo e	que sabe o a sus arc	que no chivos.	Sit	tios)
Esta zona tiene por io menos un sitio web.							
Nivel d	le seguridad pa	ara esta zona —					

Se pulsa el botón *'Sitios'* y en *'Agregar este sitio web en la zona de:'* se escribe o copia la URL anteriormente citada, marcando la casilla *'Requerir comprobación.....'* y pulsando el botón *'Agregar'*. Debería aparecer la URL introducida en la lista de *'Sitios web:'*

Sitios de	e confianza	×
✓	Puede agregar y quitar sitios web de esta zon, web en esta zona usarán la configuración de s zona.	a. Todos los sitios eguridad de la
Agrega	r este sitio web a la zona de:	
https	//webpub2.igae.hacienda.gob.es	Agregar
Sitios w	eb: ienda.gob.es	Quitar
*.mer	n.es hafp.es	
*.min	hafp.gob.es	
Req de e	uerir comprobación del servidor (https:) para to sta zona	dos los sitios
		Cerrar

Antes de iniciar el proceso, recomendable al entrar en la aplicación, se debería comprobar la accesibilidad al certificado digital. Se accede al menú *Herramientas – Opciones de Internet*, solapa de *'Contenido'* y botón *'Certificados'*, y en la pestaña *'Personal'* debería figurar el certificado que se va a usar, indistintamente de si está instalado en el navegador o en tarjeta inteligente.

5		Cert	ificados		[⇒ ×
Propósito p	lanteado: <to< td=""><td>dos></td><td></td><td></td><td></td><td>¥</td></to<>	dos>				¥
Personal	Otras personas	Entidades de cer	tificación intermedias	Entidad	des de certifica	d I
Emitido	para		Emitido por		Fecha de	Nom
	ANTON	10 - DNI 2000	AC FNMT Clase 2 CA AC FNMT Usuario AC Administración AC FNMT Usuario	s n Pú s	02/04/2016 01/04/2019 14/12/2015 08/09/2019	<nir <nir <nir <nir< td=""></nir<></nir </nir </nir
<						>
Importar	Exportar.	Quitar		O	pciones avanza	adas

Si no se tiene ningún certificado instalado en el navegador, pero se dispone de él en un fichero, habrá que instalarlo manualmente. Para ello, en la pantalla anterior (*Herramientas-Opciones de Internet-Contenido-Certificados, pestaña 'Personal'*), se pulsa en el botón *'Importar'* y se siguen las instrucciones del asistente. En lo que sigue, se comenta la importación de un certificado personal ubicado en un fichero con extensión *.pfx*, por ser el más común de ellos.

- Se pasa la primera pantalla de *Bienvenida* pulsando el botón 'Siguiente'.
- En la siguiente pantalla hay que seleccionar el fichero del certificado, pulsando en el botón 'Examinar'.

Asistente para importar certificados
Archivo para importar Especifique el archivo que desea importar.
Nombre de archivo:
Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:
Intercambio de información personal: PKCS #12 (.PFX,.P12)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Almacén de certificados en serie de Microsoft (.SST)

 En el cuadro 'Abrir' hay que ir hasta donde esté ubicado el fichero y seleccionar el tipo de fichero adecuado en el desplegable correspondiente.

	1	Abrir				×
Desktop		ע ט Bus	scar en Desktop	þ	, P]
				•		
	^	Nombre	<u>^</u>		Fecha	de
		Escaner			12/05/	201
		Maquetas virtuales			24/11/	201
		🐻 Maguinas Virtuales			24/11/	201
		Revisar			24/11/	201
		👌 Virtuales			24/11/	201
		Fisicos			09/03/	200
		👔 Guia rapida probler	mas firma		30/09/	201
		Horario			24/08/	201
		🛃 Ms Office			10/04/	201
		훩 Procesos y sistema			13/07/	201
		🛃 Pruebas papa 2015			20/08/	201
		🛃 Salidas material			25/02/	201
		🛃 Varias mias			13/07/	201
		<				>
				/* .	• • •	
		V Ce	etificado X.509	(".cer;"	".cπ) ♥	
		Int	ercambio de in	(icer; iforma	ción person	al(*
		Lis	ta de certificad	los de (confianza (*	.stl)
		Lis	ta de revocació macén de certif	on de c ficados	ertificados (serializados	(°.cı s de
		Ce	rtificados PKCS	S #7 (*.	spc;*.p7b)	
		То	dos los archivo	os (*.*)		_

 Pulsar el botón 'Abrir' y 'Siguiente'. En esta pantalla hay que introducir la 'Contraseña', que sirve para proteger la clave privada del certificado, que tiene que ser conocida (creada en el proceso de exportación detallado más adelante) y habilitar todas las 'Opciones de importación'.

ara mantener la seguridad, la clav	ve privada se protege con una contraseña.
scriba la contraseña para la clave	: privada.
ontraseña:	
•••••	
Mostrar contraseña	
pciones de importación: ✓ Habilitar protección segura c avisará cada vez que la dav ✓ Marcar esta dave como exp seguridad de las claves o tra	de clave privada. Si habilita esta opción, se le re privada sea usada por una aplicación. ortable. Esto le permitirá hacer una copia de ansportarlas en otro momento.

- Las dos pantallas siguientes se pasan con el botón 'Siguiente' y 'Finalizar'.
- El proceso mostrará una pantalla para confirmar la importación de la clave privada, se acepta y, si todo ha ido bien, se mostrará un mensaje confirmando que la importación se ha realizado correctamente.



Ahora se podrá confirmar la accesibilidad al certificado digital detallado al inicio del apartado.

Si lo que se necesita es, teniendo el certificado instalado en un ordenador, llevarlo a otro para instalarlo en este, hay que realizar el proceso de exportación del mismo a través del botón *'Exportar'* desde la pantalla de *'Certificados':*

- Como en el proceso de importación, se pasa la pantalla de Bienvenida y en la siguiente se selecciona *'Exportar la clave privada'*, pasando a la siguiente pantalla.
- En esta se seleccionan todas las opciones disponibles y se pulsa el botón 'Siguiente'.

S Asistente para exportar certificados
Formato de archivo de exportación Los certificados pueden ser exportados en diversos formatos de archivo.
Seleccione el formato que desea usar:
DER binario codificado X.509 (.CER)
🔘 X.509 codificado base 64 (.CER)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Induir todos los certificados en la ruta de certificación (si es posible)
Intercambio de información personal: PKCS #12 (.PFX)
✓ Induir todos los certificados en la ruta de certificación (si es posible)
Eliminar la dave privada si la exportación es correcta
 Exportar todas las propiedades extendidas
Almacén de certificados en serie de Microsoft (.SST)
Siguiente Can

- Se selecciona *'Contraseña'* se introduce una contraseña y se confirma. Esta contraseña sirve para proteger la clave privada que se va a exportar y que pedirá el proceso de importación antes citado.
- A continuación, a través del botón 'Examinar' se selecciona el destino del fichero resultante de la exportación, naturalmente hay que asegurarse de que el destino del fichero va a ser accesible después de terminar este proceso y se le da un nombre. La extensión del fichero la pone automáticamente el sistema (*pfx*).
- Las siguientes pantallas son iguales al proceso de importación hasta terminar con el mensaje confirmando que la exportación se ha realizado con éxito.

Pide insertar una tarjeta criptográfica

Aun teniendo el certificado instalado en el navegador, se solicita, en una ventana emergente, introducir una tarjeta criptográfica. Esto puede ocurrir si se tiene el lector de tarjetas inteligentes instalado y no se tiene ninguna tarjeta o DNIe introducido en el mismo. Hay que pulsar el botón *'Cancelar'* para que siga el proceso y poder utilizar el certificado instalado en el navegador. En ningún caso hay que cerrar la ventana desde la X blanca situada en la esquina superior derecha.

El certificado digital no se puede validar contra el certificado raíz del PSC (FNMT)

A la hora de usar el certificado digital, este no se puede validar porque falta el certificado de la entidad de certificación raíz de confianza (FNMT).

Para resolver esta incidencia hay que instalar manualmente dicho certificado raíz desde la carpeta de instalación del '*Cliente FNMT*' o '*Módulo Criptográfico*' que debe tenerse instalado según se ha visto en el apartado Escenario óptimo. Esta carpeta se suele localizar en '*C*:*Archivos de programa**FNMT-RCM*'. En

ella se encontrarán todos los certificados que proporciona la FNMT, como entidad de certificación raíz, durante la instalación de los clientes anteriores.

La lista de estos certificados es la de la siguiente imagen y la instalación de los mismos se realiza como se ha explicado en la *'Importación'* del certificado de usuario al navegador, o bien, haciendo doble-clic en cada uno de los ficheros de dicha lista y siguiendo el asistente.

o local (C:)	► FNMT-RCM
Nombre	Fecha
퉬 Configuracion Mozilla	05/10/2
ACAdministracionPublica.cer	22/04/2
ACComponentesInformaticos.cer	27/04/2
ACFNMTUsuarios.cer	24/03/2
ACRAIZAPE.cer	30/07/2
ACRAIZFNMTRCM.cer	30/07/2
FNMTClase2CA.cer	30/07/

Se recomienda instalar todos los certificados para tener una mayor seguridad.

Constitution	Coneviones Programas Opciones					_
Conexiones	Program	Briveridad	Upcio	nes avan	zadas	_
Configuración Seleccione una co Ble Ble Ble 	nfiguración para la zo poquea cookies de tero acidad sólida oquea cookies de tero tacto que se puede u estringe cookies de or tacto que se puede u Importar	ona de Internet. ceros que no tien ceros que guarda isar sin su conser igen que guarda isar sin su conser Avanzada	en un an info ntimier ntimier	a directiv rmación (nto explíc nto explíc Predete	va de de ito de ito	3
Ubicación Nunca permitir su ubicación fís	que los sitios web so sica	liciten		Borran	r sitios	
Activar el bloq InPrivate Deshabilitar ba exploración de	ueador de elementos arras de herramientas	emergentes ; y extensiones c	uando	Configu se inicie	uración la	