CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GUÍA DE USO SEGURO DE CERTIFICADOS DIGITALES

Documento Público

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Sobre CSIRT-cv

CSIRT-cv es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-cv ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2014 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana para la prevención, detección y respuesta ante incidentes de seguridad en las TICs.

Datos de contacto

CSIRT-cv Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/ Email: csirtcv@gva.es
Generalitat de la Comunitat Valenciana,
Teléfono: +34-96-398-5300
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

Licencia de uso

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Índice de contenido

1. Introducción

Tras la realización de la última campaña de concienciación respecto al uso de Certificados Digitales destinada a los ciudadanos y empleados públicos de la Comunidad Valenciana, así como por la extensión y la complejidad de la misma, desde CSIRT-cv hemos decidido construir y publicar la presente guía como resumen así como para entrar en mayor lujo de detalles en todos y cada uno de los consejos presentados en las redes sociales.

A modo de introducción y antes de comenzar con el contenido de la guía propiamente dichos, el objetivo de la campaña de concienciación es informar y concienciar respecto del uso de certificados digitales en la vida cotidiana. Se facilitan conocimientos básicos de uso de DNI electrónico, certificados digitales de firma y cifrado de correo electrónico, navegación web y certificados SSL, así como el uso de certificados en distintas aplicaciones de uso habitual en las cuales es conveniente mantener la privacidad de la información y la asegurar autenticidad del remitente o tercero con el que contactamos.

La guía se plantea con la mayor simplicidad posible y sin entrar en excesivos detalles técnicos, tratando de dar una visión realista de qué es un certificado, así como las ventajas y riesgos principales de su uso. El objetivo es ampliar los conocimientos y buen uso general de los certificados digitales, otorgando a ciudadanos y empleados públicos medios para identificar conexiones y documentos legítimos en la gran mayoría de los ámbitos; todo con el fin de hacerlos menos vulnerables a fraudes online como el Phishing o el Pharming. Dicho lo propio, comenzamos con el primero de los puntos de la guía.

2. El DNI Electrónico

El primer punto fundamental en el que nos centraremos es el certificado digital obligatorio del que disponemos todos los Españoles y que la gran mayoría desconoce... El DNI electrónico. **El DNI electrónico contiene un certificado digital emitido por una autoridad de certificación de confianza**; los usos de dicho certificado son: la identificación del interesado y la implementación de firma en entornos digitales.

2.1. ¿Qué es y para que sirve?

Como se ha comentado anteriormente, este certificado permite la autenticación y firma digital. ¿Pero esto que significa?

La principal diferencia del DNI electrónico respecto al tradicional es que **incorpora un pequeño soporte para almacenar información digital**; concretamente **almacena un certificado** digital. Del mismo modo que sucede con el propio DNI tradicional, y sumado a su funcionalidad típica; **la principal finalidad del certificado digital** contenido en el DNI electrónico **es identificar telemáticamente y de forma inequívoca al propietario del mismo**. De este modo, se facilita al conjunto de los ciudadanos un mecanismo para poder garantizar de forma remota la identidad de los interlocutores de cualquier comunicación o intercambio de datos mediante su uso.

El principal uso del DNI electrónico, y posiblemente uno de los principales motivos de su aparición es la **realización de trámites electrónicos con la administración pública**. El DNI permite a los ciudadanos realizar un amplio abanico de trámites evitando que tengan que personarse físicamente, **agilizando los mismos tanto para los ciudadanos como para la propia administración**.

Es importante destacar que adicionalmente a cualquier funcionalidad establecida y relacionada con la propia administración pública, el certificado incluido en el DNI electrónico está expedido por una Autoridad de Certificación de confianza, por lo que, **a efectos prácticos es igual de válido que otros certificados digitales de propósito general**. Este hecho permite emplear el DNI electrónico con otras finalidades, como por ejemplo:

- Realizar **transacciones seguras con entidades bancarias**.
- **Intercambiar datos con terceros en internet** teniendo total certeza de la procedencia de los mismos. Así como protegiendo su confidencialidad en el tránsito por internet.
- **Firmar digitalmente documentos**.
- **Acreditar electrónicamente la identidad de una persona**.

2.2. ¿Cómo y donde se utiliza?

Ahora que ya empezamos a tener más clara la funcionalidad del DNI electrónico, es fundamental tener claro como emplearlo. **Para emplear el DNI electrónico se deben de cumplir una serie de requisitos hardware y software**.

Los requisitos hardware, fundamentalmente, especifican que **es necesario disponer de un dispositivo lector de tarjetas inteligentes** (que siga el estándar ISO/IEC 7816). Existe una gran variedad de dispositivos de este tipo, desde internos (que están dentro del propio ordenador), hasta externos, que se conectan mediante alguno de los puertos de los que disponen los ordenadores a tal efecto, normalmente USB.

Pasando a los requisitos software, de forma general, únicamente **se necesita un ordenador personal (PC) que instale una versión de Windows XP o superior, o cualquier distribución de Linux**.

En cualquier caso dejamos a vuestra disposición información más detallada que nos facilita el Ministerio del Interior en el siguiente enlace.

Como se ha comentado con anterioridad, el uso del DNI electrónico permite el acceso a las distintas sedes electrónicas de la administración pública para la realización de un amplio abanico de trámites. A continuación **facilitamos un enlace en el que se detallan todos y cada uno de los servicios que se prestan desde todas y cada una de las sedes**.

De forma general, y para finalizar el presente punto, **facilitamos un enlace al portal web informativo que mantiene el Ministerio del Interior** para ampliar conocimientos y disponer de información adicional sobre el DNI electrónico.

3. Certificados Digitales de Persona Física

Adicionalmente al propio DNI Electrónico, **existen certificados digitales de persona física de propósito general** que nos permiten realizar las mismas acciones que el DNI electrónico y otras adicionales, como **implementar cifrado** en nuestras comunicaciones para asegurar la confidencialidad. Estos certificados **son emitidos por Autoridades de Certificación de confianza**. Si queremos obtener un certificado de dichas características, es fundamental acudir a una Autoridad de certificación de confianza en el estado Español. Para poder identificarlas, **el Ministerio de Industria, Energía y Turismo mantiene un listado actualizado de Autoridades de Certificación reconocidas** y de confianza dentro del territorio Español, os facilitamos el enlace a continuación.

Adicionalmente, estos certificados se pueden emitir con particularidades propias, como es el caso de los **certificados para empleado público**; sea como sea, **en el cuerpo de la presente guía nos referiremos a ellos como certificados de forma general**, ya que sea cual sea su uso y sus particularidades, **fundamentalmente están basados en la misma tecnología** y los usos detallados en los subsiguientes puntos se tratarían del mismo modo sea cual sea su finalidad, únicamente diferenciando entre cifrado e identificación digital, ya que éstos son empleados por aplicaciones diferentes.

3.1. Identificación digital

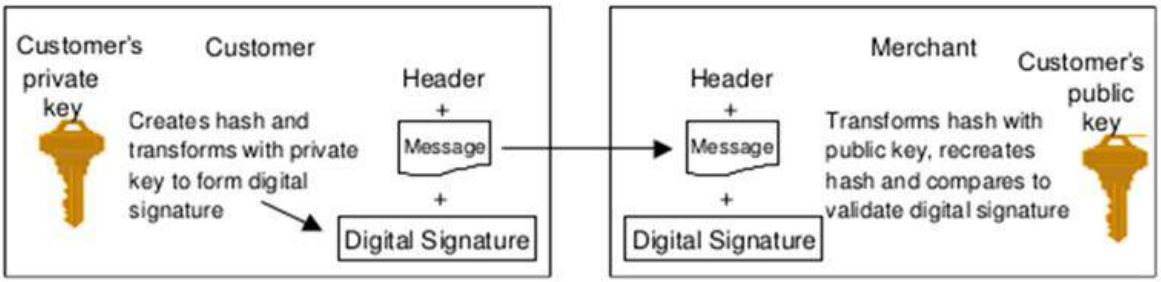
Como se ha comentado con anterioridad, una de las principales finalidades del uso de certificados digitales es la **identificación inequívoca online**. Este tipo de funcionalidad **es de uso habitual en sitios web o sedes electrónicas para dar acceso a servicios de alta sensibilidad o criticidad**.

Los certificados digitales están formados fundamentalmente por un par de claves denominadas **Clave Pública y Privada**. Dichas claves se generan mediante un **Algoritmo de Cifrado de Clave Asimétrico**, cuya principal particularidad es que, **dado un mensaje cifrado con su clave privada, únicamente podrá ser cifrado con su clave pública y viceversa**. Esta particularidad es la que permite implementar la identificación digital; para terminar de afianzar el concepto plateamos un pequeño ejemplo.

Supongamos que un usuario A quiere enviar un mensaje de correo electrónico firmado digitalmente a un usuario B; para ello, el usuario A calcula una función resumen (o también denominada de hash), mediante la cual obtiene una cadena de caracteres de longitud determinada y única en base al mensaje que se desea enviar. Tras aplicar la función, A procede a cifrar el resultado de la función de resumen con su clave privada, y anexa el resultado al final de su correo electrónico. **Este pequeño anexo constituye la firma digital del documento**.

Pasemos ahora al otro lado, B recibe el mensaje por su parte y procede a ir deshaciendo todas las acciones previas; en primer lugar procede a descifrar la firma digital con la clave pública de A, y en segundo lugar calcula la función resumen del correo y la compara con el resultado que ha descifrado de la firma digital. Si al comparar los valores son iguales, B **está asegurando dos puntos fundamentales**, en primer lugar que **el mensaje efectivamente proviene de A**, ya que si ha descifrado el mensaje con su clave pública implica que necesariamente debe haber sido cifrado con su clave privada; y en segundo lugar, **asegura la integridad del mensaje**, ya que si hubiera sido modificado, los resultados de los dos cálculos de la función resumen habrían sido distintos.

Para ilustrar el ejemplo planteamos el siguiente diagrama resumen:



Una vez comprendemos como funciona el mecanismo para la identificación digital, **el siguiente paso es aprender a usar vuestra firma digital**. Para ello, **es necesario instalar vuestro certificado de persona física en las herramientas que requiráis**, como por ejemplo un navegador; de este modo cuando se intente acceder al sitio web, el navegador ofrecerá emplear el certificado como medio de autenticación. A continuación facilitamos unos **consejos para la instalación y protección de certificados en los principales navegadores comerciales**. Los consejos se dividen por el navegador web que empleemos.

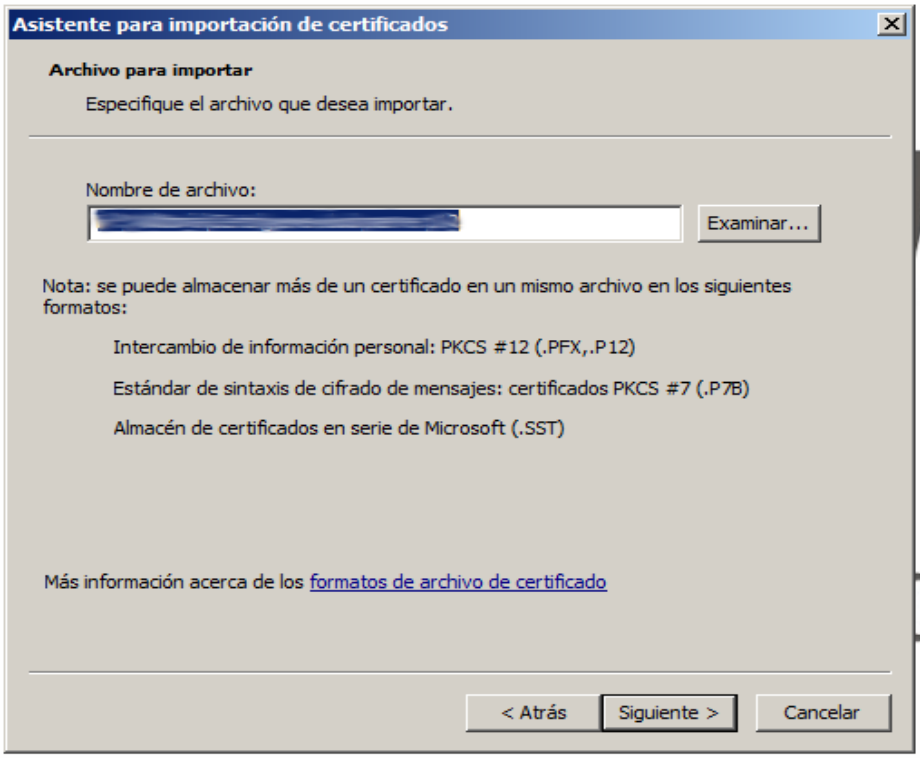
Antes de comenzar con dicha separación, comentaremos los puntos comunes en ambos casos. **Cuando se obtiene un certificado de persona física en soporte software, lo habitual es que se entregue en un fichero de tipo .p12**. Este tipo de fichero es un contenedor cifrado que almacena el certificado, y **requiere de una contraseña para poder instalarlo**; en caso de que no dispongas de ella ponte en contacto con tu Autoridad de Certificación para subsanar el problema.

Es importante distinguir el certificado digital en soporte software del resto, como por ejemplo el DNI electrónico; **un certificado en soporte software se entrega sin ningún tipo de soporte**; es decir, no se mantiene en ningún dispositivo físico (tarjetas, tokens USB, etc.). A lo largo de la presente guía se dará información adicionalmente sobre certificados digitales alojados en soporte hardware.

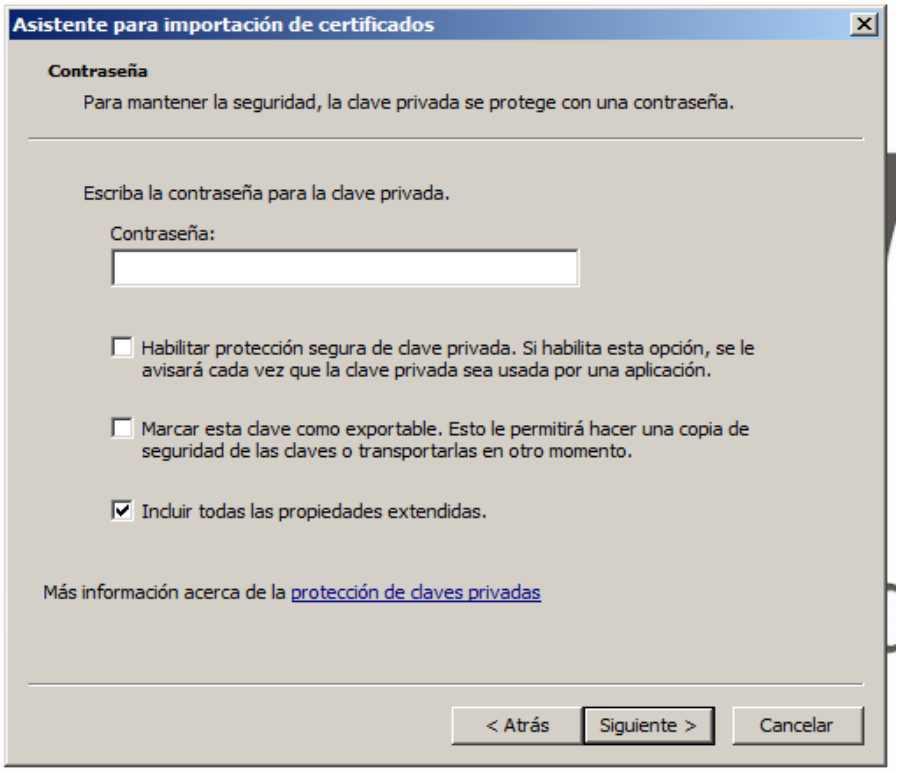
3.1.1. Internet Explorer

Para **instalar el certificado en Internet Explorer** el proceso es muy sencillo, únicamente deberemos hacer doble clic sobre el archivo .p12, y se abrirá una ventana de asistente de importación de certificado semejante a la que se muestra a continuación.

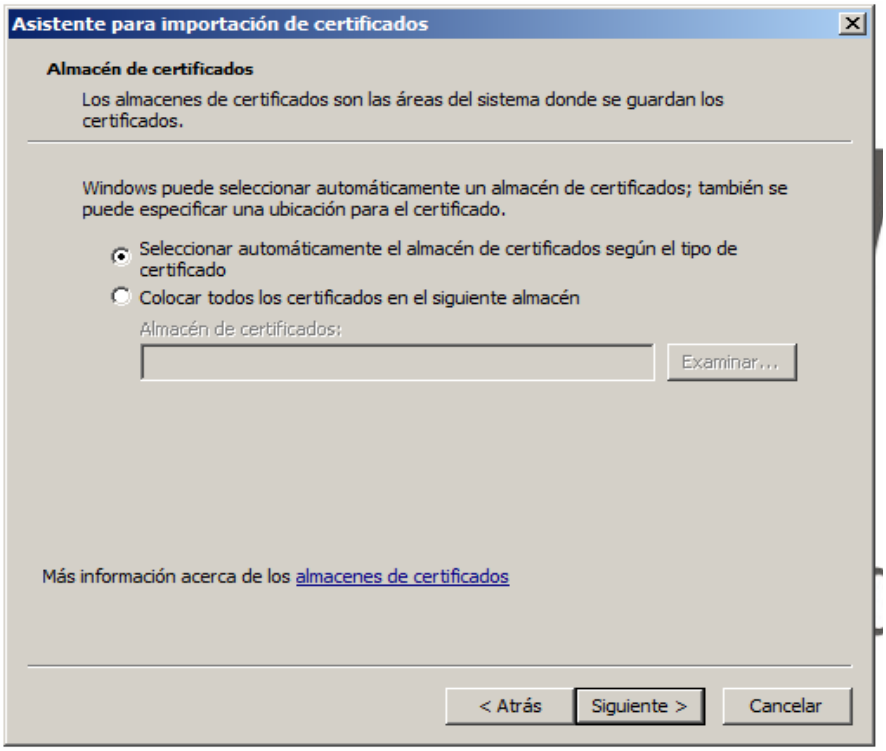
Pulsamos en *Siguiente* y se nos mostrará el siguiente formulario.



Debe aparecer la ruta en la que se ha almacenado el .pkcs12, en ese caso, se hace clic en *Continuar*.



En este formulario **se debe introducir la contraseña que debe habernos facilitado la Autoridad de Certificación**, y permite el acceso a las claves del certificado que contiene el archivo .p12. Adicionalmente, recomendamos que se aplique la opción "*Habilitar protección segura de la clave privada*", de este modo se recibirá una notificación cada vez que se emplee el certificado con cualquier fin. Una vez hemos cumplimentado los campos podemos proseguir haciendo clic en *Siguiente*.



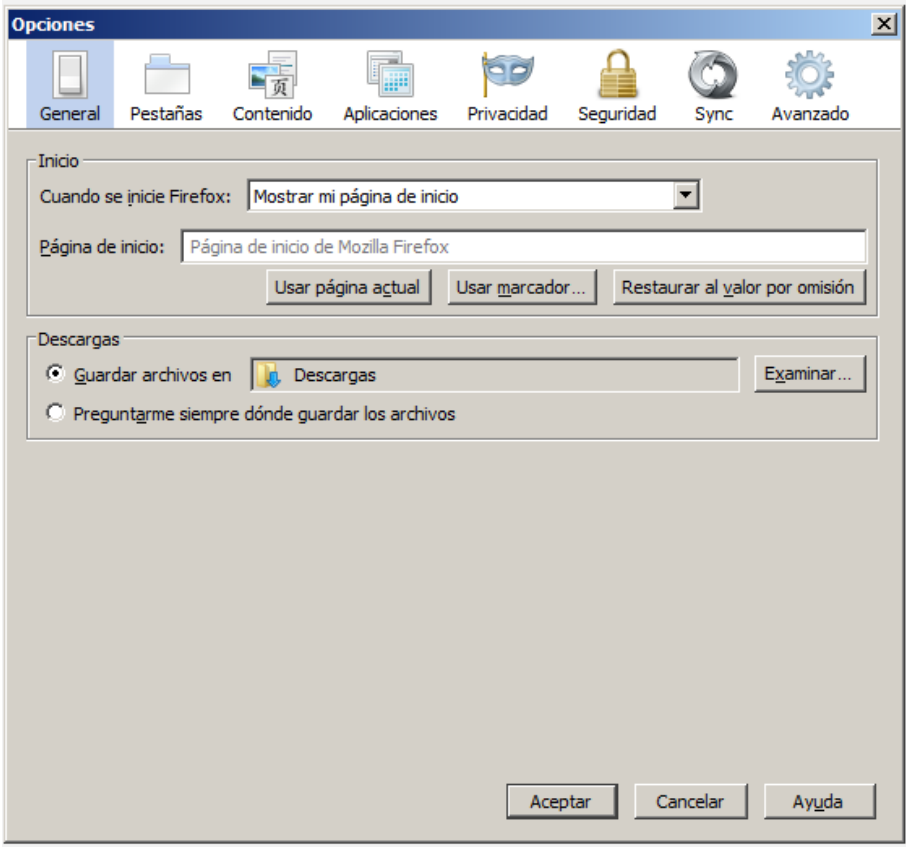
Mantenemos las opciones definidas por defecto y volvemos a hacer clic en *Siguiente*. Lo que nos lleva a la pantalla directa de finalización del proceso, **tras esto, el certificado estará correctamente instalado para su uso con Microsoft Internet Explorer**.

3.1.2.

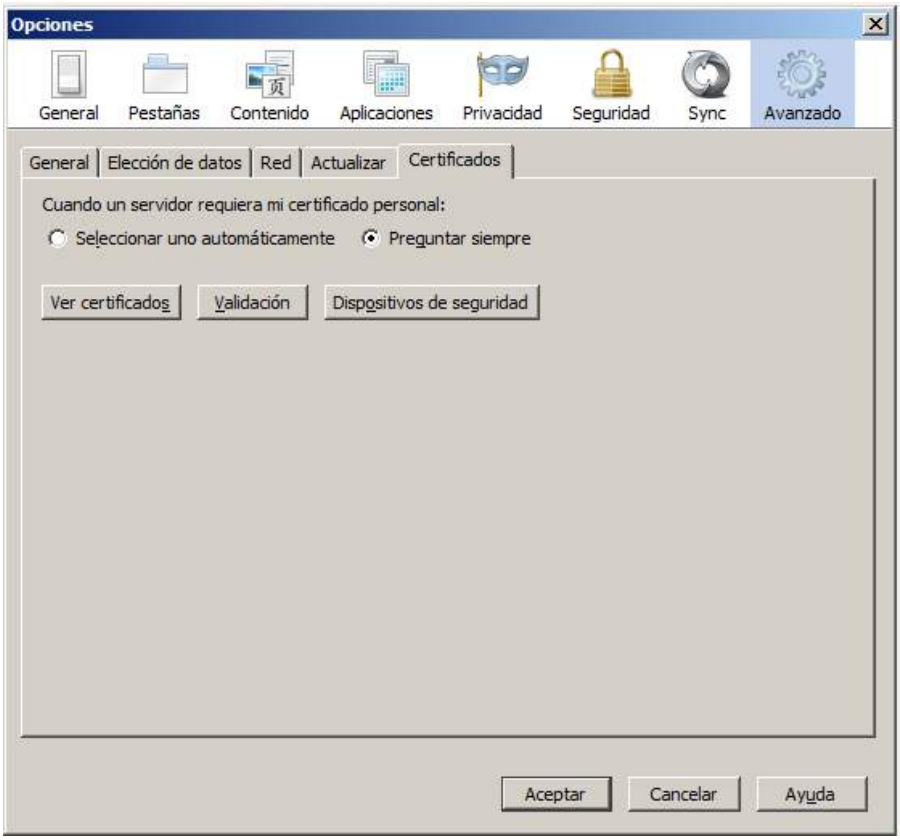
Mozilla Firefox

En este caso vamos a proceder a realizar la **instalación del certificado en Mozilla Firefox**, para ello, y del mismo modo que en el caso anterior, proponemos una serie de pasos a seguir.

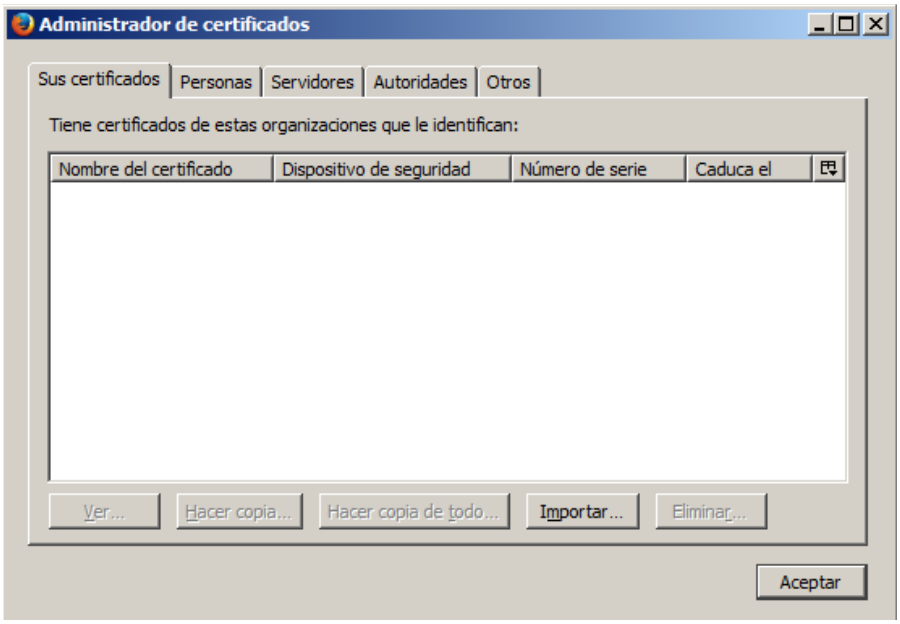
El primer paso es abrir el navegador, y acceder al siguiente menú *Herramientas* → *Opciones*; en caso de que no puedas identificar el menú de herramientas pulsa la tecla ALT para mostrar la barra de menú en la parte superior de la ventana. Accederemos al siguiente menú.



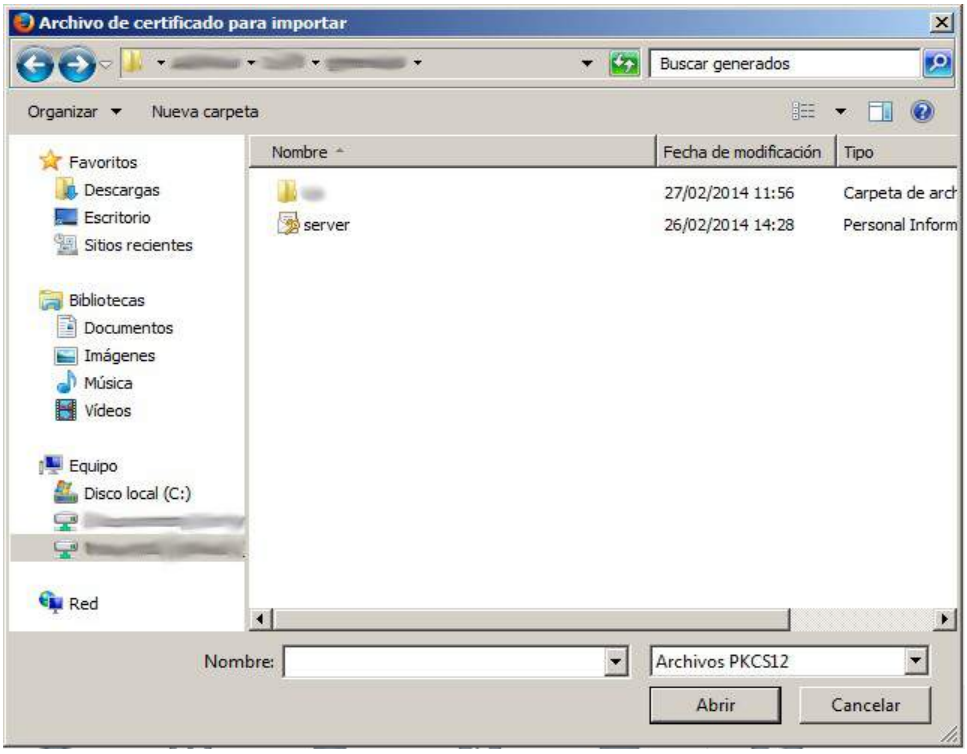
Dentro de la ventana, debemos seleccionar *Avanzado* → *Certificados* → "*Ver certificados*". Tal y como se muestra a continuación.



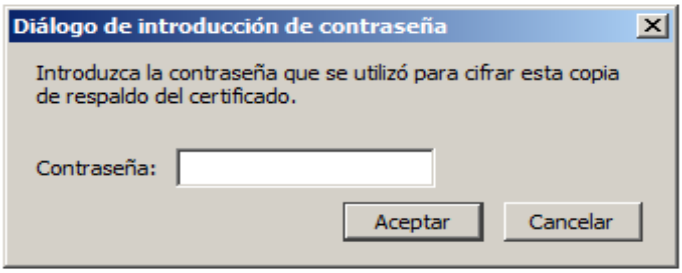
Tras realizar la selección se nos mostrará la siguiente ventana, en la que debemos situarnos en la pestaña "*Sus certificados*" y a continuación pulsar sobre el botón *Importar*.



En la siguiente ventana, se debe buscar y seleccionar el archivo PKCS#12 (extensión .p12) que contiene el certificado digital que se desea instalar y seleccionarlo.



La única información que nos quedaría por cumplimentar en este caso será la clave que protege el archivo PKCS#12, para que de este modo se instale adecuadamente en el navegador.

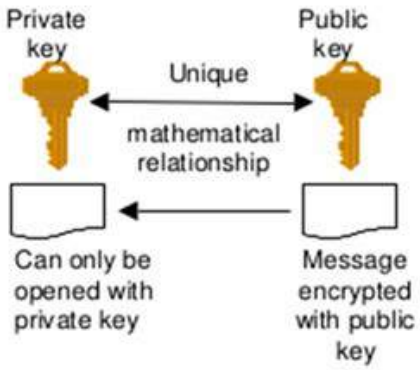


3.2. Cifrado

Del mismo modo que sucede con la implementación del la firma digital, **los certificados digitales se pueden emplear para cifrar información**. Procediendo del mismo modo que en el punto precedente, se plantea un ejemplo para facilitar la comprensión del concepto.

En este caso, el usuario B desea enviar información cifrada a A, para ello, y una vez tiene construido el mensaje, lo cifra empleando la clave pública de A. Una vez lo ha cifrado lo envía por el canal que considere oportuno, ya que el mensaje está cifrado y garantiza la confidencialidad de la información remitida.

El usuario A, por su parte, recibe el mensaje y lo descifra empleando su clave privada; pudiendo acceder al mismo sin problemas. El **mensaje se ha transmitido de forma segura**, y basándonos en las particularidades del cifrado asimétrico, **el único que podrá descifrar el mensaje será el propio destinatario**; y lo que es más importante; **sin necesidad de transmitir una clave de cifrado entre ambos**, lo que podría suponer un riesgo de seguridad si ésta fuera interceptada. Se muestra un pequeño diagrama resumen de la explicación anterior:



Se facilitarán nociones para la instalación de certificados de firma o cifrado en el correo electrónico para cifrado y autenticación en puntos posteriores de la presente guía, concretamente en el punto dedicado al correo

electrónico.

3.3. Revocación

Tal y como se ha comentado en puntos anteriores, **siempre que se tenga la más mínima sospecha de que un certificado digital de nuestra propiedad o de la de cualquiera, debemos notificar inmediatamente a la Autoridad de Certificación emisora del certificado afectado**, así como solicitar su revocación. Si no lo hacemos, **un ciberdelincuente podría suplantar la identidad del propietario del certificado**, empleando su certificado digital. Sin que este hecho sea detectable o trazable.

Hay que tener en cuenta que **este certificado, aunque se haya vulnerado, a nivel operativo es perfectamente válido**, por lo que **la única forma existente para poder comprobar si un certificado emitido ha sido revocado es consultando a la propia Autoridad de Certificación**.

Cada autoridad de certificación tiene medios o canales distintos para recibir este tipo de notificaciones. En el Anexo del presente documento se dan detalles pormenorizados para la solicitud de revocación de certificados pertenecientes a la **Agencia de Certificación de la Comunidad Valenciana (ACCV)**.

Adicionalmente, se facilitan enlaces a los mecanismos que mantiene la **Fábrica Nacional de Moneda y Timbre (FMNT)**, considerada Prestador de Servicios de Certificación de confianza dentro del estado Español.

Notificación - https://www.sede.fnmt.gob.es/certificados/persona-fisica/anular

Consulta - http://www.cert.fnmt.es/catalogo-de-servicios/validacion-de-certificados

3.4. Certificados digitales en soporte hardware

Durante el desarrollo de la siguiente guía, se ha tratado la instalación y uso de certificados digitales, alojados en un soporte software (concretamente dentro de un contenedor PKCS#12); sin embargo, **los certificados también se pueden entregar y usar empleando un dispositivo hardware**, como una llave USB o una smart card.

Es muy habitual que, en estos certificados que se encuentran alojados en dispositivos hardware se empleen **mecanismos de seguridad** como por ejemplo un **PIN para proteger el contenido del dispositivo** (básicamente para proteger el par de claves pública/privada que constituyen el certificado). Estos códigos PIN, del mismo modo que el código PIN de un teléfono móvil, **se bloquean tras un determinado número de intentos de acceso a las claves fallidos**, bloqueando indefinidamente el uso del certificado alojado en el dispositivo.

Para poder **recuperar el dispositivo** y el contenido en estos casos, este tipo de dispositivos **emplea un código de seguridad PUK**, también como pasa con los dispositivos móviles, que permite desbloquearlo.

Dado que cada Autoridad de certificación puede optar por una marca o modelo de dispositivo u otro, **las instrucciones concretas sobre la obtención de los códigos PIN y PUK dependerá directamente de la propia Autoridad**.

Referimos de nuevo en este caso al Anexo de información sobre certificados de ACCV; así como se facilita información al respecto para la FMNT; se detalla en el siguiente enlace.

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

4. Uso de Certificados Digitales en Correo Electrónico

El siguiente punto de fundamental dentro de la presente guía está dedicado al **correo electrónico**, el **medio de comunicación de uso más difundido en internet**. Del mismo modo que cualquier medio de comunicación digital que transmite datos por redes públicas requiere que se tengan en cuenta los requisitos de seguridad pertinentes; y como suele ser habitual, centrados en la **confidencialidad de la información** compartida, así como la **autenticidad** de la misma.

Dados estos requisitos, es muy habitual el uso de certificados digitales en el correo electrónico, dado que **se trata de un protocolo no seguro en su concepción**, que envía por defecto la información intercambiada en claro. Debido a esto, una **configuración adecuada del correo** es fundamental para poder garantizar la **seguridad de la información** intercambiada, así como la propia **seguridad de nuestro equipo**; ya que es uno de los medios de uso más común para la realización de acciones maliciosas directas contra los usuarios, como podrían ser campañas de phishing o envíos de malware.

A este respecto, y con el fin de mejorar el uso general de los ciudadanos de esta herramienta de comunicación, **CSIRT-cv ha publicado un** micro curso de uso seguro del correo electrónico; en la que se detallan ampliamente medidas de seguridad aplicables a este medio de comunicación y que quedan fuera del alcance de la presente guía, en la que el objetivo principal es el uso de certificados digitales en cualquier ámbito.

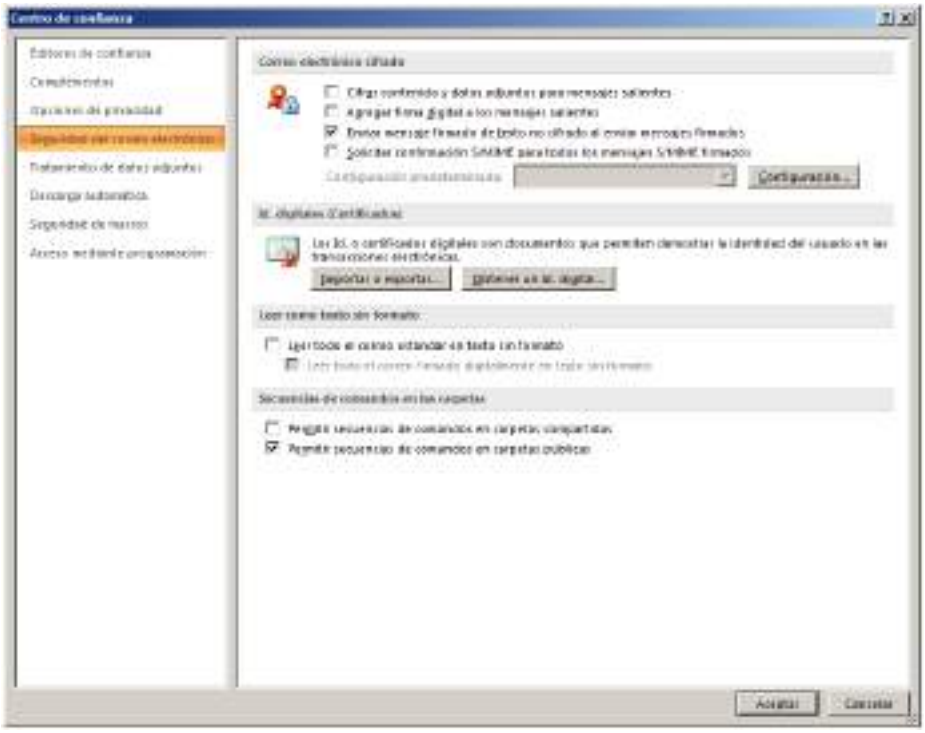
Como se ha comentado con anterioridad, se va a repasar la **instalación y uso de certificados digitales dentro de los principales clientes de correo comerciales**, para facilitar su uso. Es importante destacar que la instalación de certificados que se va a detallar es **válida para la instalación tanto de certificados de cifrado como de firma digital**.

4.1. Microsoft Outlook

En primer lugar, se va a mostrar como instalar un certificado digital personal que permita la firma de correos electrónicos salientes con nuestra propia firma, o bien recibir correo cifrado de otros destinatarios empleando también nuestro certificado digital. En un segundo apartado, más breve, se detallará como instalar la clave pública de un tercero, de modo que se pueda enviar correo electrónico cifrado empleando certificados digitales al mismo.

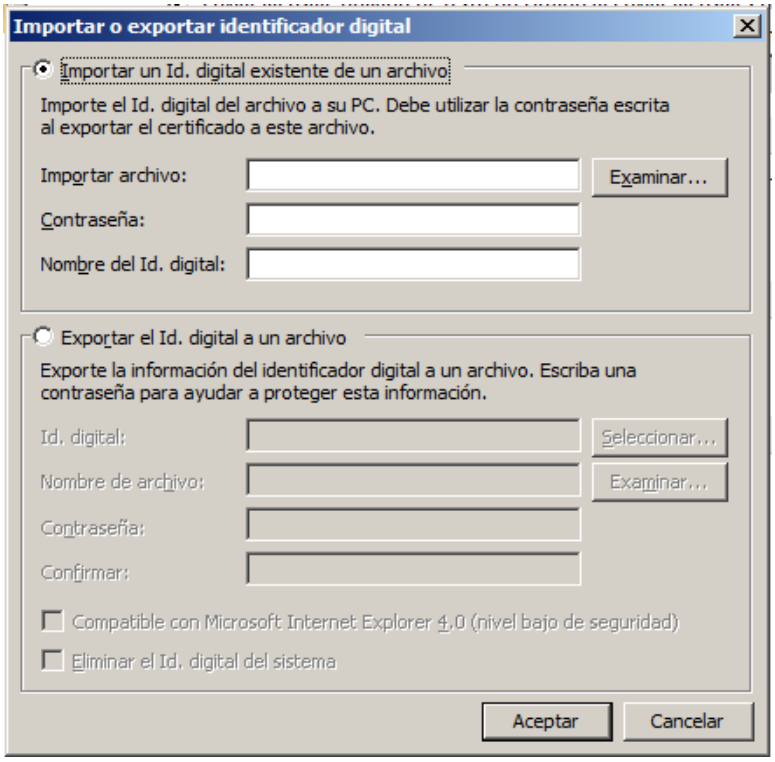
Instalación de Certificados Digitales Propios

Para instalar un certificado digital de persona física propio, es decir, su clave pública y privada, se debe acceder al menú *Herramientas* → "*Centro de Confianza*" → "*Seguridad del Correo Electrónico*", se muestra una captura del menú al que deberíamos acceder a continuación.



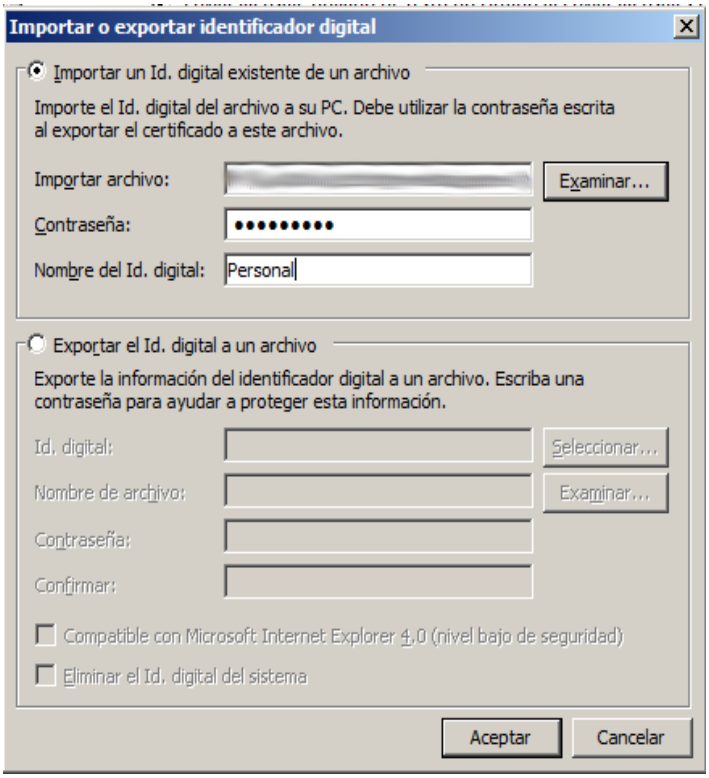
El siguiente paso será hacer clic en el botón "*Importar o Exportar*",

accediendo al siguiente menú.



Se puede observar que se muestran dos menús diferenciados: en el primero, se dan opciones para poder añadir un Identificador Digital, y en el segundo se facilitan opciones de acceso, eliminación y exportación a un fichero de los que ya están instalados. Para el caso que nos ocupa, deberíamos seleccionar "*Importar un Id. digital existente de un archivo*" y a continuación pulsar en "*Examinar*".

Una vez en la ventana de navegador, se debe seleccionar la ubicación en la que se encuentre nuestro certificado en formato .p12 y seleccionarlo, lo que nos devolverá al menú anterior. Solo quedaría completar la contraseña para el acceso al .p12 y especificar un identificador para el Id digital, para facilitar su identificación dentro del repositorio. Debería quedar como sigue.



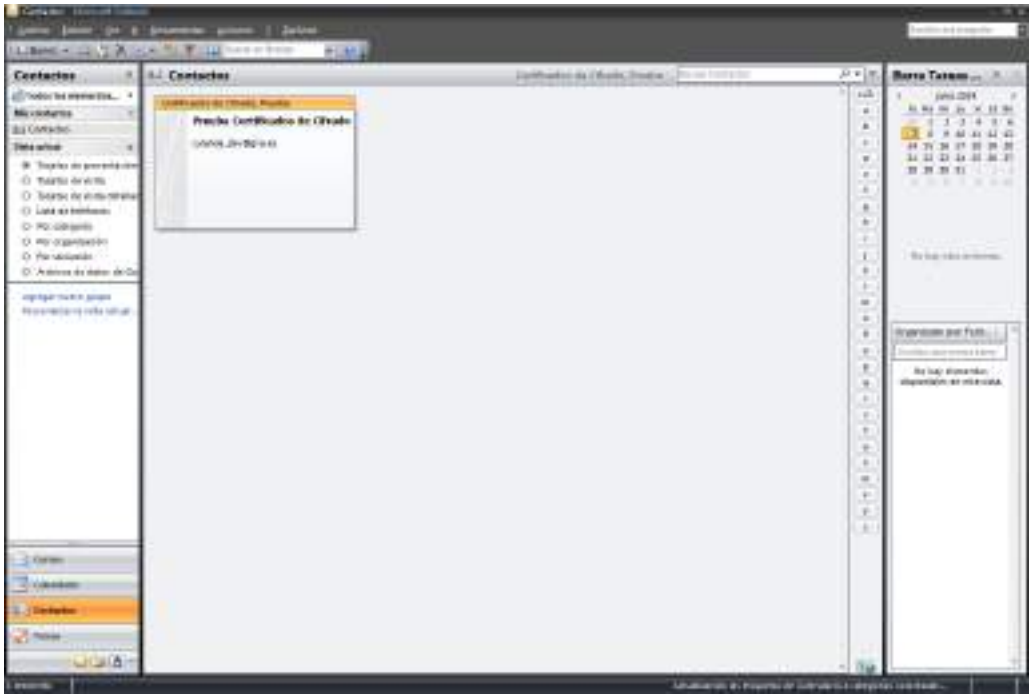
Una vez cumplimentados todos los campos, se debe hacer clic en Aceptar, dando por concluida la instalación del certificado.

Importación de Claves Públicas de Terceros

Para realizar la importación de claves públicas de cifrado correspondientes a terceros, **Outlook nos facilita dos medios diferenciados**.

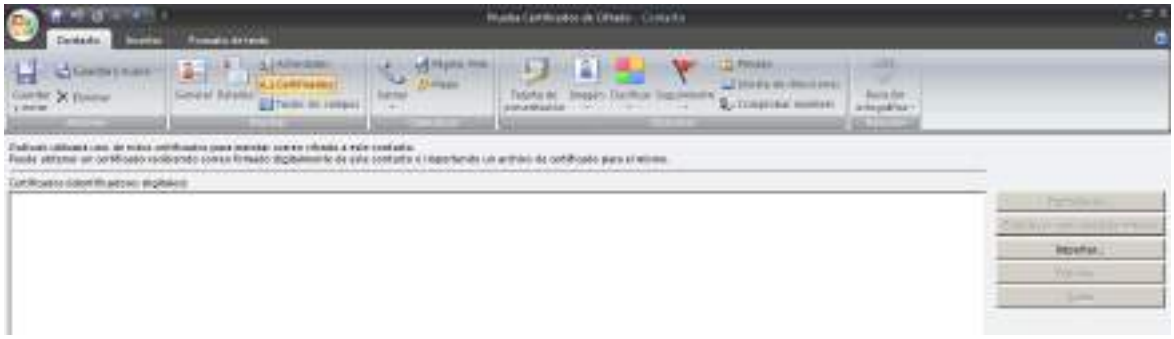
El **primero** de ellos cuenta con que el propietario de dichas claves nos las envíe como adjunto en un correo electrónico. En ese caso, sobre el correo que adjunta las claves, deberemos hacer clic con el botón derecho del ratón sobre el campo *De* (en el que aparece el remitente del correo), y en el menú contextual que aparecerá se debe pulsar sobre "*Agregar a Contactos*" en caso de que no se haya definido el contacto en la agenda de Outlook, y a "*Actualizar el contacto existente con la nueva información*" si ya se ha incluido.

Para el **segundo** de los casos, suponemos que se desea instalar el certificado desde un archivo de certificado (.crt), para ello debemos acceder al apartado *Contactos*.



Abrir el contacto para el que queremos instalar el certificado.

Y pulsar sobre el botón *Certificados*.



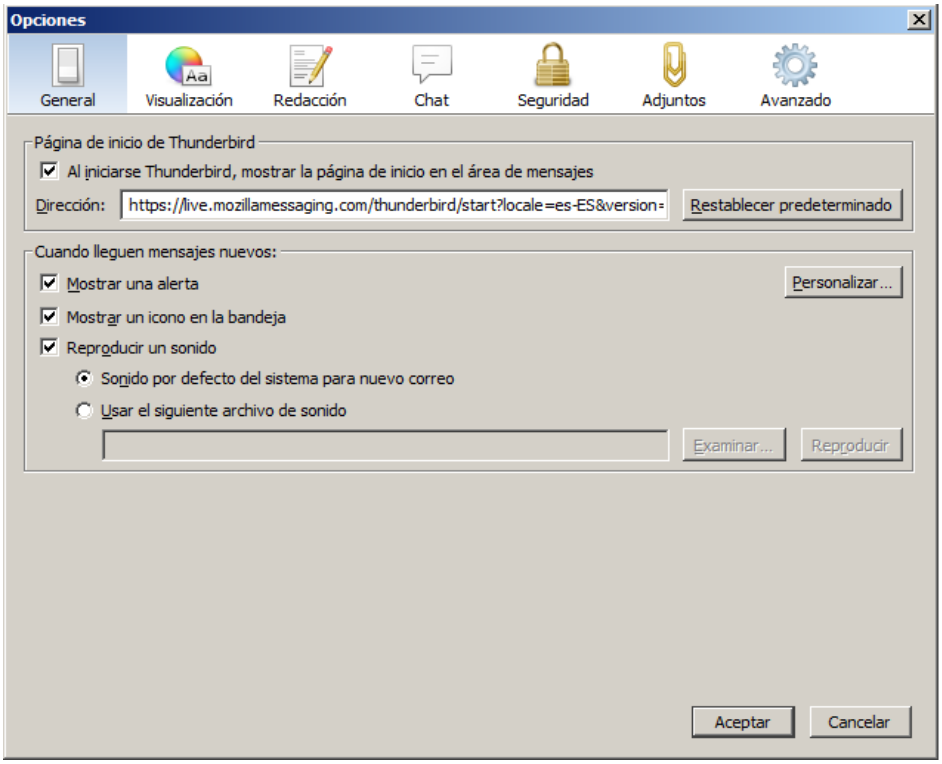
Para finalizar el proceso seleccionar el botón *Importar...*, tras ello se nos mostrará una ventana para la selección del certificado a instalar el archivo que mantiene el certificado. Una vez seleccionado se instalará para su uso. Sea cual sea el método empleado, tras ello podremos enviar correo cifrado empleando certificados digitales para el remitente seleccionado.

Es importante destacar que **se puede configurar el cliente de correo para que incluya la firma digital en todos los mensajes salientes**, o bien se puede especificar en cada uno de los mensajes redactados si incluir la firma digital o no. La configuración de la firma digital en correo se puede encontrar en *Herramientas* → "*Centro de Confianza*" → " *Seguridad del Correo Electrónico*"; concretamente en el apartado "*Correo electrónico cifrado*".

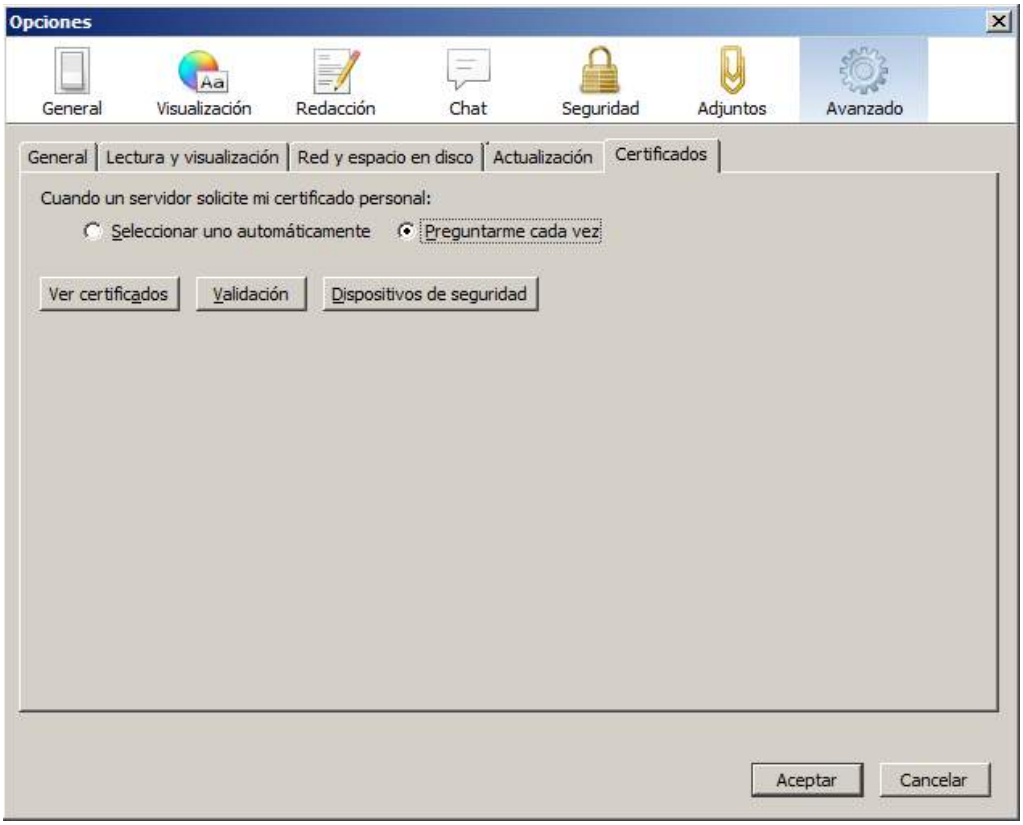
4.2. Mozilla Thunderbird

A continuación se detallan los pasos para proceder a la instalación de un certificado digital de firma o cifrado en el cliente de correo **Mozilla Thunderbird**.

En primer lugar se debe acceder a *Herramientas* → *Opciones* , tras lo que se mostrará una ventana como la que sigue.

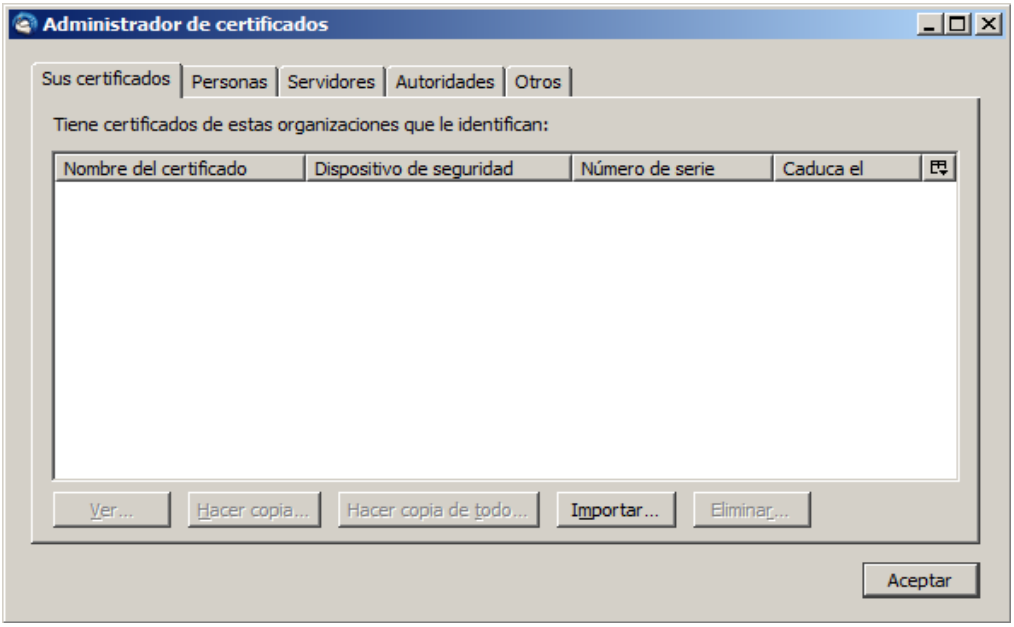


A continuación, debemos acceder al apartado *Avanzado* y a la pestaña *Certificados* dentro del mismo.

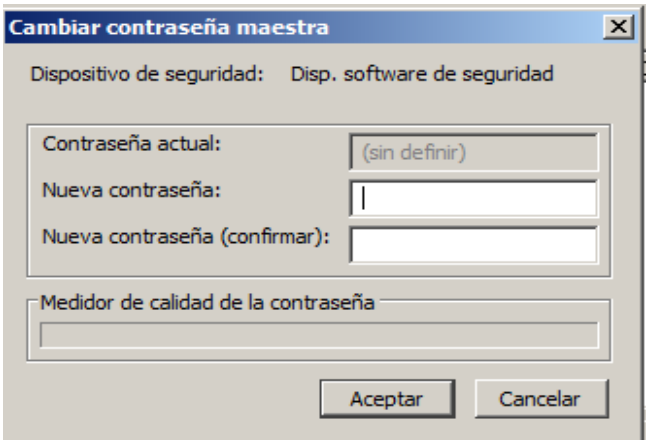


Instalación de Certificados Digitales Propios

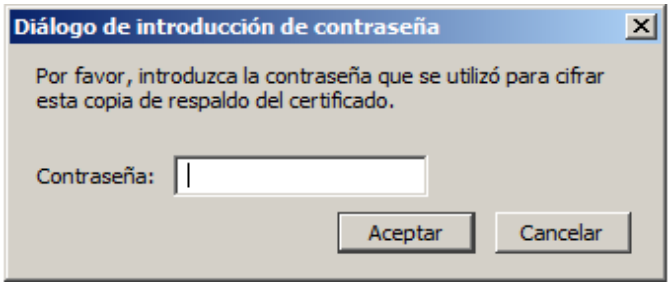
El siguiente paso es hacer clic sobre el botón "*Ver Certificados*", y acceder a la pestaña "*Sus certificados*", en la que se listan todos los certificados digitales instalados en el cliente de correo.



Para importar un nuevo certificado digital, debemos acceder al menú *Importar...*. En el que se nos mostrará una ventana del explorador de archivos donde deberemos acceder a la ruta de acceso al archivo .p12 que contiene el certificado digital. Si es el primer certificado que se importa a la herramienta, lo habitual es que nos **solicite establecer una contraseña maestra** mediante la cual se protege todo el repositorio de certificados del cliente de correo, es fundamental que dicha contraseña sea robusta (al menos 8 caracteres, y uso de letras mayúsculas, minúsculas, números y signos de puntuación). Un buen indicador de la calidad de la contraseña se nos muestra al introducirla mediante la barra de "*Medidor de calidad de la contraseña*" cuanto mas alto sea el valor más robusta será la misma.

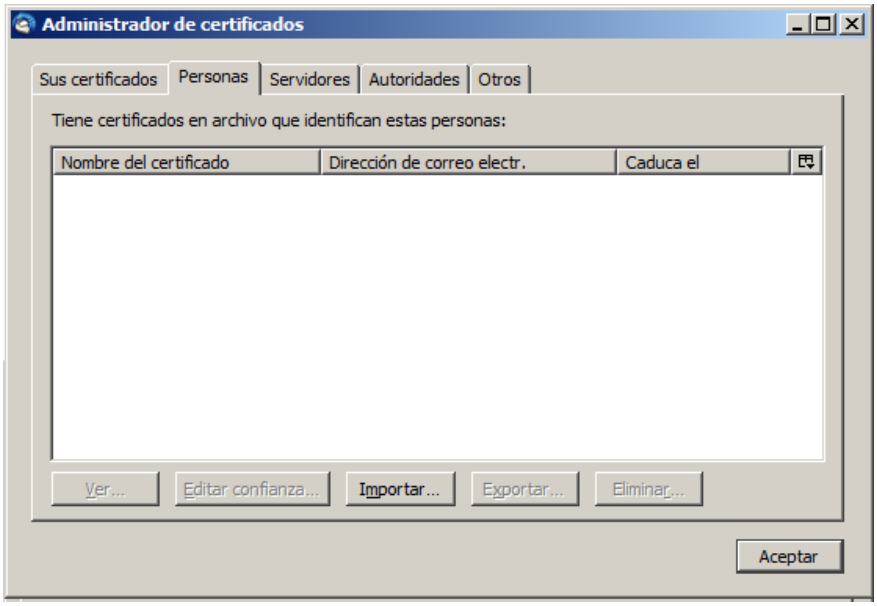


Una vez seleccionado, se nos mostrará la siguiente ventana, en la que sí que **será necesario que se introduzca la contraseña que protege el certificado que deseamos instalar** (la facilita la Autoridad de Certificación emisora), tras aceptar; el certificado estará instalado y listo para su uso. Quedando listado en el apartado "*Sus certificados*" y listo para su uso.



Instalación de Certificados Digitales de Terceros

Para proceder a instalar certificados digitales de terceros en este caso se debe realizar disponiendo de la clave pública de cifrado del destinatario en un fichero, una vez nos encontramos dentro del menú "*Administrador de Certificados*" debemos pulsar sobre la pestaña *Personas*, y a continuación en *Importar*. Se describe el acceso a esta parte del programa en el principio de esta sección.



A continuación la aplicación nos mostrará un diálogo en el que deberemos indicarle la ubicación del certificado, una vez hecho esto dispondremos del certificado completamente instalado y listo para remitir correos cifrados al destinatario propietario del mismo.

4.3. Alternativas para firma y cifrado de correo

Como hemos comentado con anterioridad, el uso de un certificado para identificación digital requiere de una Autoridad de Certificación que lo emita y valide su autenticidad. Cuando se recibe un certificado que no está emitido por una Autoridad de Certificación, puede ser muy complicado para el receptor de un mensaje firmado asegurar la identidad del remitente; sin embargo, **en entornos conocidos o si la finalidad es exclusivamente implementar cifrado, se pueden emplear medios alternativos que permiten generar y gestionar certificados digitales en nuestro propio equipo**. Con fines identificativos esto es posible única y exclusivamente si conocemos la procedencia del certificado emitido, aunque no se trate de una autoridad de certificación de confianza reconocida.

Para realizar este tipo de actividades destacamos **herramientas como**

GNUPG. GNUPG es un software de código abierto multiplataforma que facilita en gran medida la generación y gestión de certificados digitales. Otra de las ventajas de este software es que se encuentra **ampliamente soportado por los clientes de correo comerciales más empleados**, así como emplea una **tecnología similar a la que emplean las Autoridades de Certificación** para generar los certificados digitales; aportando obviamente un nivel de confidencialidad semejante.

Para los usuarios de **Windows**, recomendamos emplear **GPG4win**, una adaptación de GNUPG propia para sistemas operativos de Microsoft. Podéis descargarla y ver la documentación relacionada en la página del proyecto.

Los usuarios de sistemas **Linux** disponen de la **herramienta de forma nativa**, en caso contrario, se podrá instalar directamente del repositorio correspondiente a la distribución que empleen. Para más información os remitimos a la página del proyecto (en inglés).

Por último, mencionar un plugin que facilita la integración de CNUPG con Mozilla Thunderbird o Seamonkey llamado **Enigmail**, este complemento permite la creación y gestión de certificados GNUPG de una forma sencilla para el uso de los mismos con correo electrónico. Dejamos a vuestra disposición el enlace a la página oficial del proyecto; en cualquier caso, este plugin se puede descargar directamente de los repositorios de complementos de las herramientas compatibles.

5. Navegación segura

Como se ha ido mostrando a lo largo de la presente guía, **los certificados constituyen un medio de identificación orígenes de datos**, así como para proteger la propia información en tránsito. En el ámbito de la navegación web no iba a ser distinto; ya que del mismo modo que se puede emitir un certificado digital para una persona se puede emitir un certificado para un sitio web (Certificado SSL).

Algunos sitios web implementan la tecnología de certificados mediante el **protocolo SSL**. Dicho protocolo **emplea certificados digitales para identificar inequívocamente al sitio web al que nos conectamos y a su vez implementa cifrado entre todas las comunicaciones entre cliente y servidor**. La aplicación de estas medidas debería ser un requisito siempre y cuando un sitio web solicita información del usuario, desde un acceso a una **parte privada** de la web mediante el uso de usuario y contraseña, hasta páginas web que manejen **datos sensibles** del usuario, como podrían ser **datos de carácter personal o financieros**.

La implementación del protocolo SSL en un sitio web se denota por el uso de el protocolo HTTPS en su ruta de acceso. Como por ejemplo:

https:*//www.ejemplo.com/*

Antes de introducir cualquier información en un sitio web **se debe comprobar** que dicho sitio web implementa HTTPS, ya que **en caso contrario toda la información intercambiada con el sitio web se transmitirá sin ningún tipo de cifrado**, viajando los datos en claro por internet; lo que facilitaría a un ciberdelincuente la captura y acceso de los mismos.

Adicionalmente, y como se ha comentado, el uso de HTTPS se basa en

certificados digitales, por lo que el certificado digital de un sitio web no sólo se emplea para cifrar la información, sino que sirve a su vez para **asegurar que el sitio web al que nos hemos conectado es legítimo**.

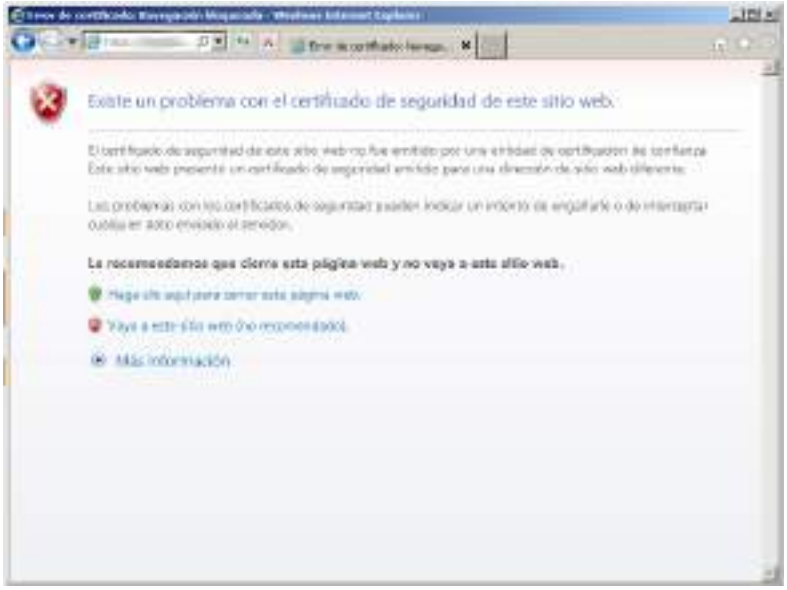
Puede que a los ojos del lector este hecho sea un tanto confuso, ya que cuando nos conectamos a un dominio en internet siempre se tiene la sensación de estar conectándose al sitio adecuado. Esto no siempre es así, en la red se dan gran cantidad de estafas, de modo que **los ciberdelincuentes engañan a los usuarios** para conectarse a sitios web fraudulentos e idénticos a los originales con el fin de **obtener credenciales de acceso** a servicios críticos como podrían ser accesos a banca online, redes sociales, etc. Con esta información los ciberdelincuentes pueden **suplantar la identidad** de los usuarios en este tipo de servicios, incluso obtener información suficiente como para obtener acceso a otros; así pudiendo realizar todo tipo de acciones maliciosas.

5.1. Navegación segura

Servicios que manejan información crítica como plataformas de pago o banca electrónica **deben implementar cifrado HTTPS** y mantener un **certificado digital de confianza**. Cuando vayamos a realizar una conexión contra servicios de este tipo **nunca deberíamos recibir ningún mensaje de error del certificado**. En caso que se produzca algún problema recomendamos que os pongáis en contacto con el proveedor del servicio empleando un medio alternativo, como por ejemplo el teléfono.

En general, **los navegadores** comerciales implementan **mecanismos destinados a identificar este tipo de fraudes o problemas**, basándose en la legitimidad de certificados digitales; obviamente, **cae en el lado del usuario entender y tratar adecuadamente cualquier advertencia relacionada**, ya que siempre se facilita la posibilidad de conectar a un sitio potencialmente peligroso si el usuario lo decide así. Se incluye una captura de ejemplo de estas no notificaciones para cada uno de los navegadores

comerciales de mayor uso en la red, Internet Explorer y Mozilla Firefox respectivamente.



Dejamos un par de enlaces a vuestra disposición con **información detallada respecto a todos los errores de validación de certificados** que puede dar cualquiera de los navegadores planteados.

Internet Explorer - http://windows.microsoft.com/es-es/windows/certificate-errors#1TC=windows-7

Mozilla Firefox - https://support.mozilla.org/es/kb/Esta%20conexi%C3%B3n%20no%20est%C3%A1%20verificada

Es fundamental entender cuánta información y de que importancia y criticidad se maneja cuando se accede a un sitio web. **Cuanta más crítica sea la información que se vaya a emplear** o a enviar sea **más inflexible se debe ser con las medidas de seguridad que implementa el sitio web**, así como con la **verificación de la identidad** del sitio.

Una buena recomendación para evitar caer en estafas de **phishing**, es **evitar acceder a sitios web conocidos mediante enlaces** que se nos puedan facilitar en los correos electrónicos. Los hiperenlaces que se incluyen en los correos pueden omitir información a simple vista, de modo que nos podemos conectar a dominios fraudulentos si no somos precavidos.

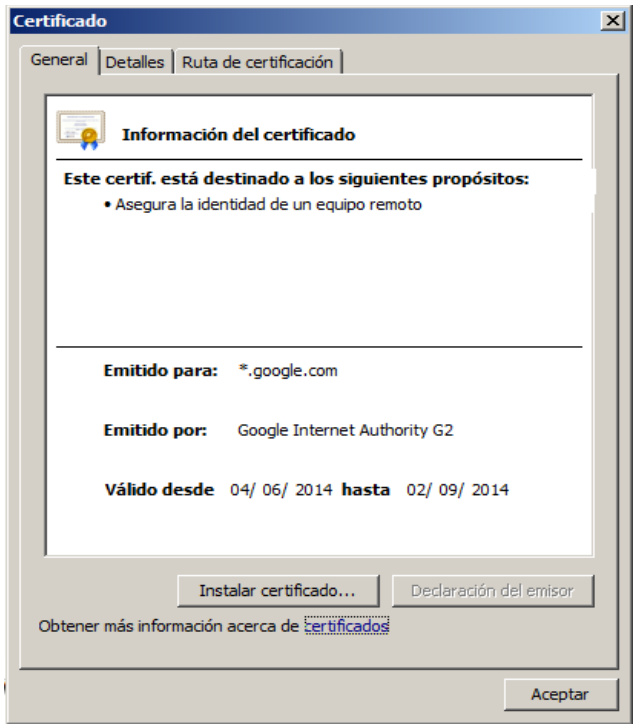
Otro punto fundamental a tener en cuenta cuando se está verificando la legitimidad de un sitio web que emplea SSL es la **caducidad del certificado** digital implementado. Los certificados digitales, como si de un DNI tradicional se tratara, tienen una fecha de vigencia. Lo habitual es que si se da esta situación, los navegadores comerciales que se emplean de forma cotidiana nos **muestren alertas** semejantes a las mostradas en capturas de pantalla anteriores.

En caso de no ser así, se puede **verificar el certificado manualmente**, ya que los navegadores comerciales incluyen visores estándar de certificados digitales. Se detalla a continuación como obtener dicha información en los de uso más extendido.

5.1.1. Internet Explorer

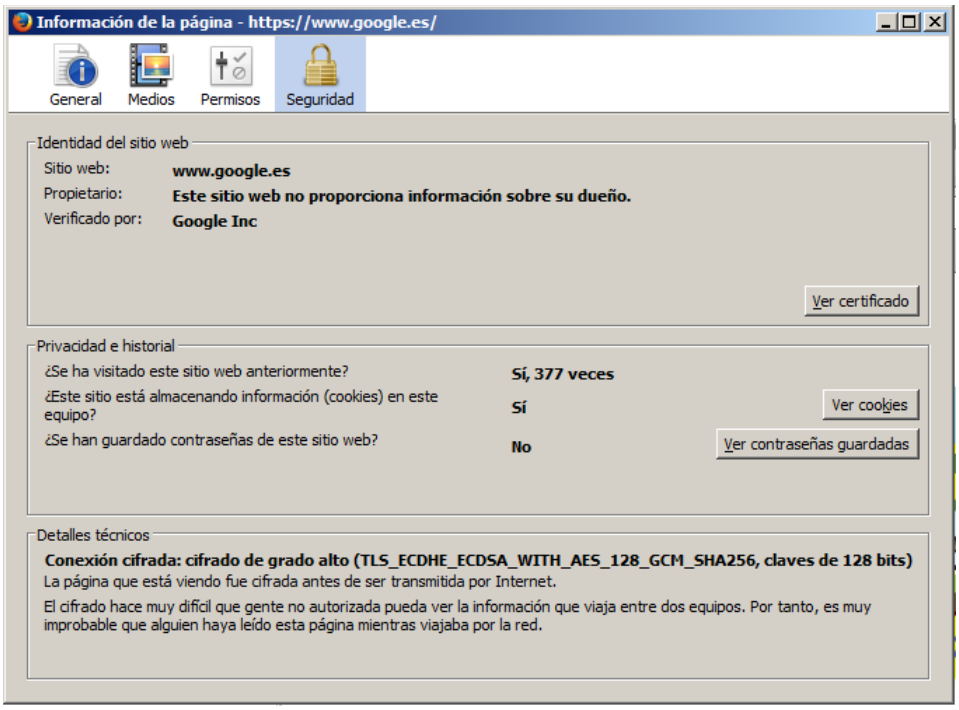
Pulsando sobre el candado que denota que se ha establecido una

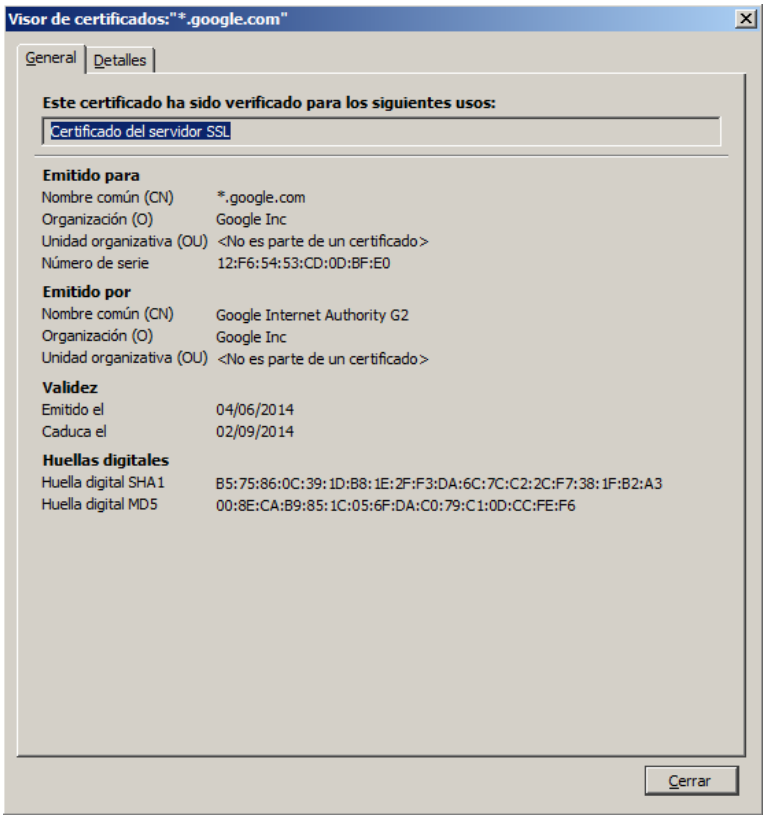
conexión HTTPS, se puede acceder a la información del certificado mediante el botón "*Ver Certificados*", como se muestra en las capturas.



5.1.2. Mozilla Firefox

Del mismo modo, pulsando sobre el candado, a continuación en "*Más información*" y por último en "*Ver Certificado*", se obtiene la misma información, se muestra a continuación:





Adicionalmente, y como se ha comentado con anterioridad, **los certificados digitales pueden ser vulnerados**. En este caso, es posible que el propietario legítimo del mismo no tenga constancia de que el

certificado ha sido vulnerado. Si se diera la situación, un ciberdelincuente podría suplantar la identidad de un sitio web legítimo, y **nosotros no tendríamos modo alguno de averiguarlo** con la única observación del certificado.

Cuando se tiene la sospecha de que un certificado digital ha podido ser vulnerado, se sea o no el propietario del mismo, **se debe contactar con la autoridad de certificación responsable** notificando el problema y solicitando su revocación. Con el fin de informar a los usuarios de certificados digitales de su responsabilidad, las Autoridades de Certificación mantienen mecanismos online en tiempo real para la validación de dichos certificados. En el siguiente enlace se facilita información adicional, así como unas sencillas instrucciones para asegurar que tu navegador está correctamente configurado para comprobar la validez de los certificados.

En cualquier caso, si con los mecanismos que incluyen los navegadores web o con las verificaciones manuales planteadas no estamos del todo seguros de la legitimidad de un sitio web, siempre podemos recurrir a herramientas externas como la que nos facilita **SSLLabs**, que mantiene una **sistema online de validación de certificados SSL de sitios web**. Únicamente es necesario introducir el dominio que queremos analizar recibiremos un diagnóstico completo y fiable del estado del certificado digital asociado. Se facilita un enlace a continuación con una explicación del servicio junto con las instrucciones de acceso.

Para finalizar, y con el fin de ayudaros con éstas y otras cuestiones, os recomendamos el siguiente minicurso publicado por CSIRT-cv sobre Seguridad en la Navegación.

5.2. Consideraciones propias para otros sitios web que manejan información sensible

Adicionalmente a los servicios de banca electrónica o pago online, existen muchos otros **servicios que gestionan una gran cantidad de información sensible** que es conveniente proteger, como por ejemplo los motores de búsqueda por internet.

Google mantiene cifrado mediante HTTPS en su **motor de búsqueda**, y lo fuerza en las conexiones; sin embargo, otros motores como Bing no fuerzan el uso de cifrado. Verifica qué tipo de conexión realizas cuando accedes a estos websites de páginas y **asegura que implementan HTTPS**, esto además de proteger tu información te permitirá asegurar una conexión legítima con el servicio al que se desea acceder. Comprueba que tu motor de búsqueda implementa HTTPS si quieres garantizar la privacidad de tu información.

Todos estaremos de acuerdo en que las **redes sociales** acumulan una **gran cantidad de información personal**, y en algunos casos estos sitios web no facilitan por defecto la seguridad de la información en tránsito. Twitter o Tuenti fuerzan el uso de HTTPS por defecto en la actualidad, pero Facebook no. Asegura tener bien configurados a las redes sociales o sitios en los que se almacene o gestione información personal para evitar disgustos habilitando cifrado. Os facilitamos las instrucciones para configurarlo en Facebook en el siguiente enlace.

Adicionalmente, y a pesar de que no tiene relación directa con el objeto de esta guía, recomendaros la siguiente guía publicada por CSIRT-cv respecto a Privacidad en Facebook que os puede ayudar a proteger vuestra información personal alojada en la red social.

Otros servicios para los cuales deberíamos revisar el tipo de conexión

que establecemos son los relacionados con **almacenamiento en la nube**. Del mismo modo que en otros servicios que manejan información de los usuarios, es fundamental comprobar el certificado del servidor para asegurar su identidad, **asegurar que se implementa HTTPS** y revisar las condiciones del servicio para ver las responsabilidades del proveedor respecto a la información almacenada. Este tipo de información se puede encontrar en los sitios web de cada uno de los proveedores, podéis revisar las de Google Drive, Dropbox y Box:

Google Drive - http://www.google.com/policies/terms/

Dropbox - https://www.dropbox.com/terms

Box - http://box.com/static/html/terms.html

Otro de los puntos principales de atención que no podemos pasar por alto las aplicaciones de mensajería instantánea para móviles. **Whatsapp** implementa cifrado SSL empleando certificados digitales, aunque en una variante de cifrado (RC4) que se determinó como vulnerable, por lo que desaconsejamos enviar o recibir ninguna información sensible con esta aplicación. Como ayuda para emplear Whatsapp con seguridad, os referimos a nuestra campaña de concienciación al respecto en el siguiente enlace.

Siguiendo con certificados digitales y mensajería instantánea, pasamos a la protección de la **mensajería en los ordenadores personales**. En este caso, os recomendamos emplear **Pidgin**, un cliente de código abierto y funcional para la mayoría de plataformas como *Google Talk*, *MSN* o *Facebook Chat*. Su uso con el plugin **OTR** (*Off the Record*) asegura la privacidad y autenticidad de tus conversaciones empleando certificados digitales. En el siguiente enlace podréis encontrar un tutorial detallado para instalar y emplear ambas herramientas.

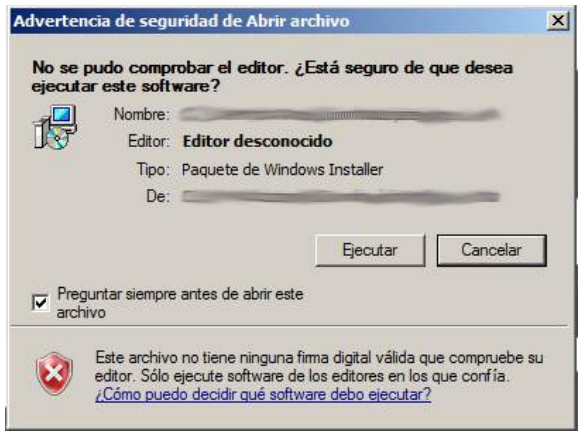
6. Firma de Código

Otro de los usos habituales de los certificados es la **firma de código**, esta capacidad permite firmar código fuente de las aplicaciones que vamos a instalar en nuestros equipos. **Cuando un código no está firmado o no está firmado por una entidad de confianza corremos el riesgo de que se haya modificado fraudulentamente**, y muy posiblemente pueda ejecutar acciones maliciosas en nuestros ordenadores. Cada vez que instalemos un programa deberíamos asegurar su origen, integridad y su legitimidad.

Esta funcionalidad es útil desde cualquier programa que haya que instalar en nuestros equipos, por ello, el propio sistema operativo **Windows**, mantiene un sistema de validación de firma de códgio ejecutable denominado ***Authenticode***. Este sistema se encarga de **analizar la firma aplicada a cualquier ejecutable o instalador** que el sistema intenta lanzar, y **realiza advertencias** cuando existe alguna irregularidad en los mismos.

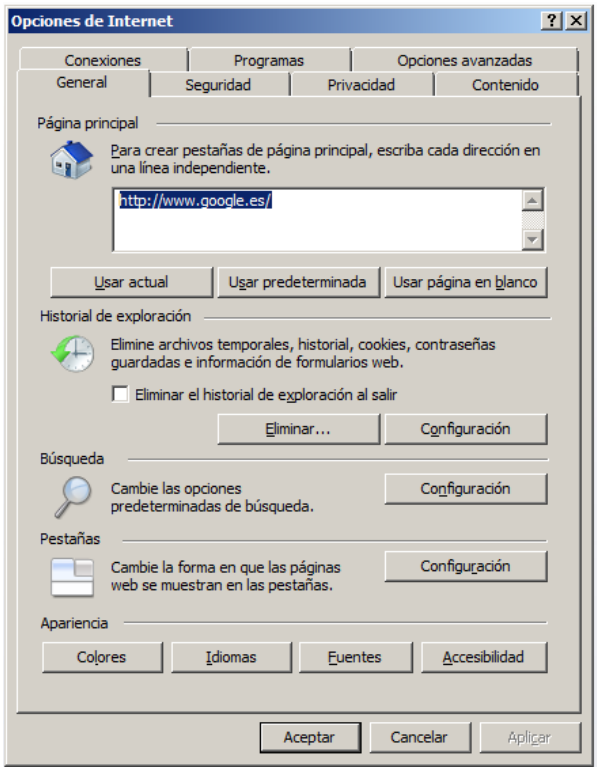
Funciona con certificados digitales, y basándose en el mismo mecanismo, **aceptará como válidas la firmas de código implementadas con certificados digitales emitidos por Autoridades de Certificación de Confianza**, y que se encuentren en el repositorio que el sistema operativo mantiene a tal efecto.

Un ejemplo de una captura de pantalla que podría generar este mecanismo relacionado con la firma de código sería el siguiente:

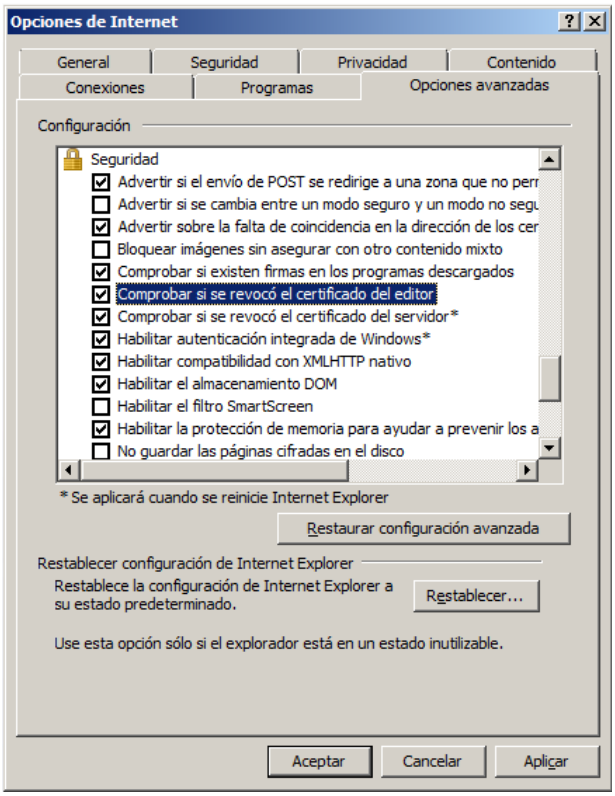


Como podemos observar en la captura, *Authenticode* nos indica que la **el ejecutable no está firmado**, por lo que **no puede certificar el origen y legitimidad del programa**. En caso de que la aplicación disponga de una firma digital válida y emitida por un editor de confianza este mensaje no se mostrará.

Para **asegurar que está habilitada** esta funcionalidad se debe acceder, dentro de Internet Explorer, acceder a *Herramientas* → *Opciones de Internet*. Se nos mostrará la siguiente ventana:



Después debemos acceder a la pestaña de *Opciones Avanzadas*, y dentro del apartado *Seguridad* asegurar que se encuentra marcado el valor *Comprobar si se revocó el certificado del editor*, se muestra el valor en la siguiente captura:



Es importante destacar que en muchos casos, y aunque no debería de ser así, **aplicaciones legítimas no van firmadas**, **no son firmadas con certificados de confianza**, o tienen una **firma no válida**. Cuando se reciba un mensaje de este tipo se recomienda, al menos asegurar la procedencia del software; en caso de tener cualquier duda **no instalar** y **ponerse en contacto con el desarrollador** o proveedor del mismo.

Otro punto en el que es fundamental la firma de código es el **código en la web**, este caso es si cabe aún mas peligroso dado que los scripts de este tipo se ejecutan en muchos casos durante la navegación, y son transparentes al usuario. De entre las aplicaciones que se ejecutan en los sitios web, **Java** es la de uso más extendido. Para advertir a los usuarios, **el software de Java permite identificar código sin firmar, o firmado por entidades de baja confianza**. Se muestra a continuación una captura de ejemplo de un error de certificado de firma de código generado por Java:

Dejamos también a vuestra disposición el siguiente enlace en el que se describen de forma pormenorizada los mensajes que puede generar la validación de firma de código fuente de Java, así como las acciones recomendadas.

7. Firma de Documentos

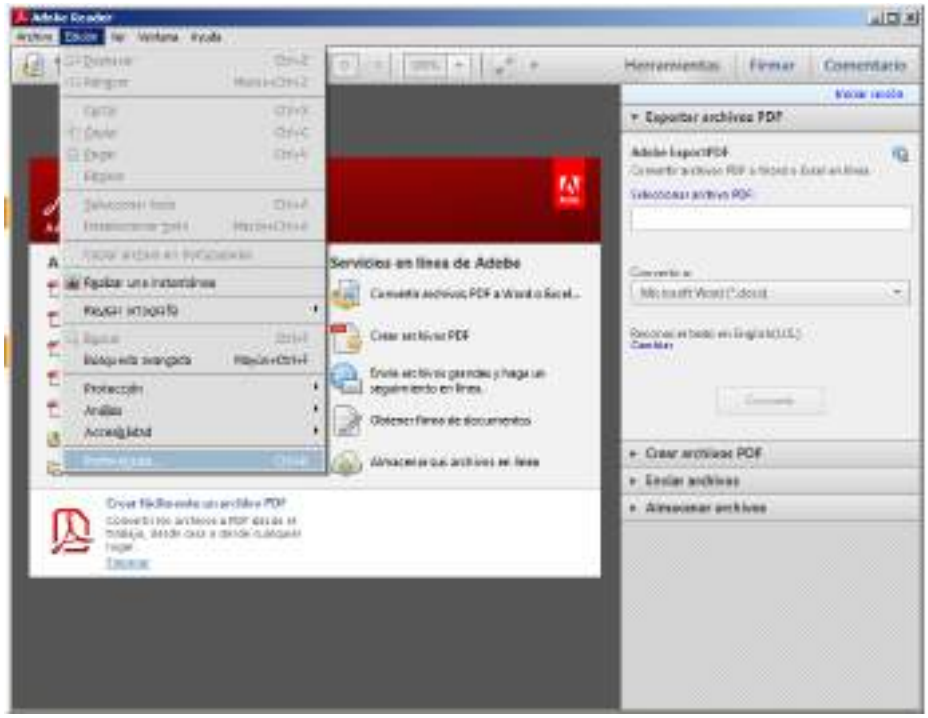
Otro uso común y conocido de los certificados digitales es la **firma de documentos digitales**. Cuando se firma un documento digital, dicha firma **tiene la misma validez que una firma manuscrita**; además asegura **que el documento firmado no ha sido alterado o modificado**.

Para facilitaros la posibilidad de firmar un documento digital, os vamos a detallar unos sencillos pasos para proceder, por una parte a instalar vuestro certificado digital con la herramienta **Adobe Reader**, y por otra parte, a firmar propiamente los documentos.

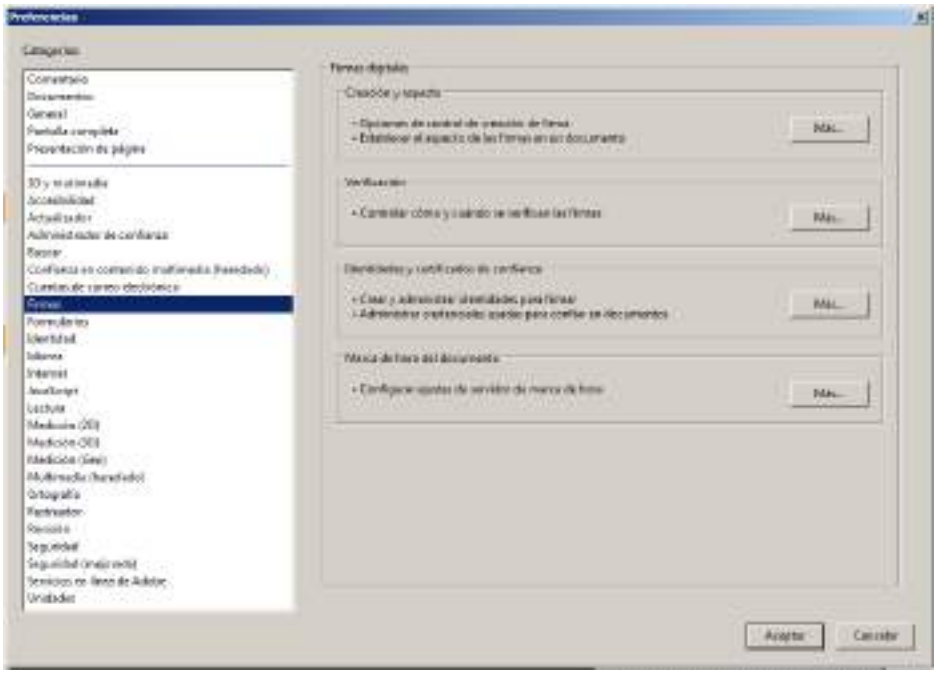
7.1. Instalación de certificados en Adobe Reader

Como se ha realizado en los anteriores tutoriales, el primer paso para poder emplear un certificado digital en una herramienta es proceder a su **instalación**. Para ello procedemos a detallar unos sencillos pasos ilustrados con capturas de pantalla de todo el proceso para la herramienta Adobe Reader.

En primer lugar, se debe acceder al menú de *Edición* de la aplicación, y a continuación acceder a *Preferencias*:

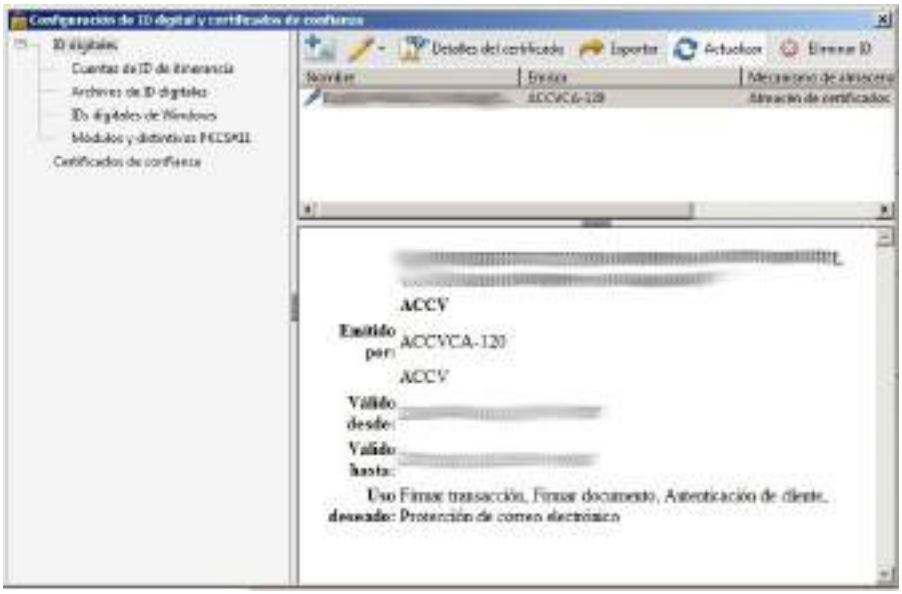


Una vez accedamos se nos mostrará la siguiente ventana, en la que deberemos acceder al panel de *Firmas*:



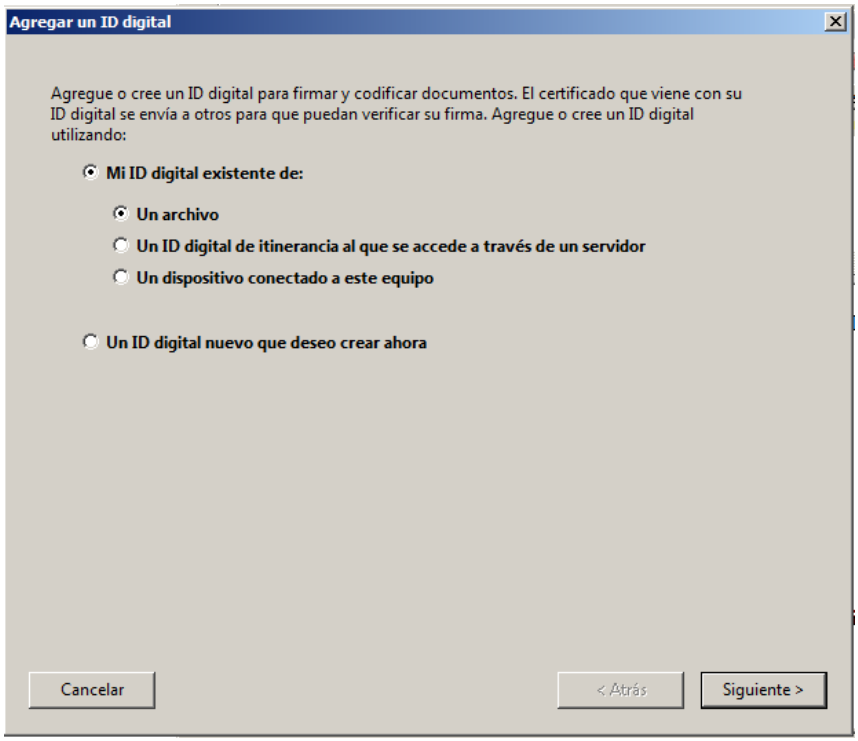
Una vez en el panel, se debe acceder dentro del apartado "*Identidades y certificados de confianza*" y pulsar en el botón *Más*, a lo que se nos mostrará

el siguiente diálogo:

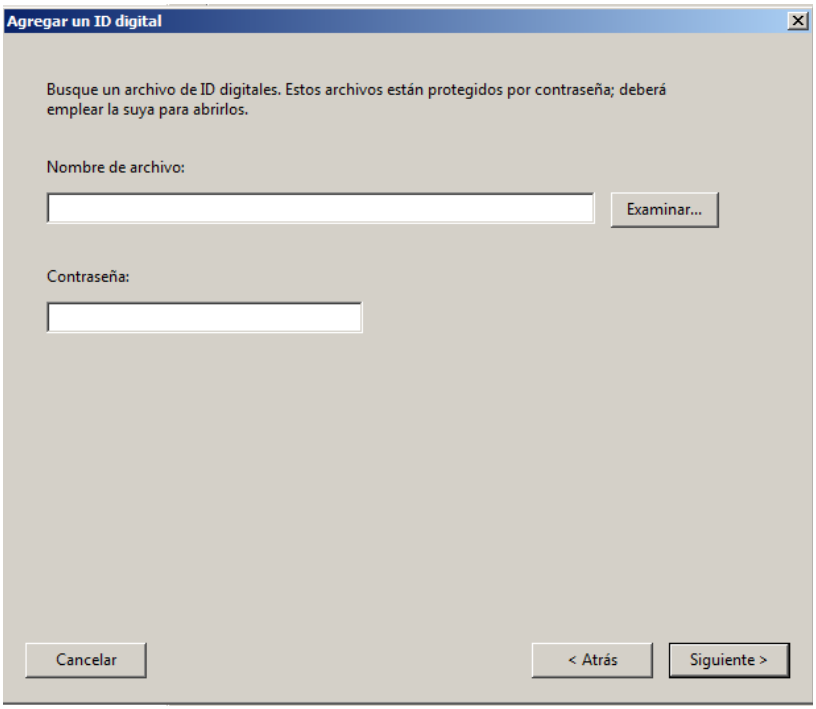


Dentro del apartado de "*ID digitales*" se muestran la totalidad de las firmas instaladas en el sistema; es importante destacar que Adobe Reader recoge los certificados digitales que están instalados en el repositorio del sistema operativo, por lo que es posible que si ya se ha instalado el certificado para su uso en con Microsoft Outlook o Internet Explorer no sea necesaria su instalación.

Si es necesaria la **instalación del certificado** se deberá hacer clic sobre el siguiente icono, llevándonos a la captura de pantalla de a continuación:



Lo habitual es que la firma se importe desde un **archivo** (.pkcs12), por lo que se debe dejar marcada la opción por defecto y pulsar en *Siguiente*:

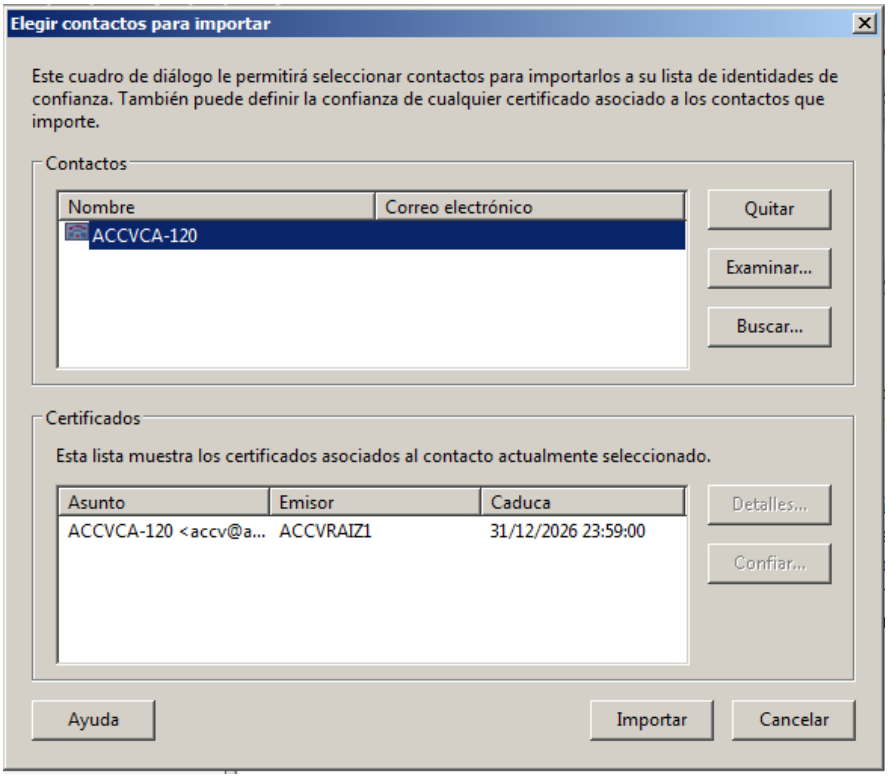


En la siguiente ventana deberemos indicar al programa la ubicación del archivo que contiene el ID digital, así como la contraseña que lo protege, tras esto, únicamente se mostrará una ventana con la información del certificado a importar, tras su confirmación habremos instalado el certificado satisfactoriamente.

Tras la realización de estas acciones, **es posible que se identifique algún problema con la firma**, habitualmente (aunque esto dependerá del la Autoridad de Certificación que emite al certificado), debidos a que Adobe Reader no considera el certificado de confianza, para ello, **será necesario instalar los certificados propios de la Autoridad de Certificación**, que suelen estar a disposición pública en el sitio web de la misma. En la presente guía se introducen cuestiones concretas sobre los certificados de ACCV en el Anexo a la misma, en caso de que el certificado empleado pertenezca a otra, se recomienda consultar directamente a la misma en caso de duda.

En cualquier caso, supongamos que ya disponemos de los certificados propios de la CA, para **instalarlos** debemos seguir los siguientes pasos. En primer lugar, y dentro de la ventana de ID Digital, debemos acceder en este caso al apartado "*Certificados de confianza*", mostrándose los certificados de confianza correspondientes a CA que mantiene instalados la herramienta:

Para añadir el certificado, una vez descargado y alojado en nuestro equipo, debemos pulsar sobre el icono *Importar*, obteniendo el siguiente diálogo.



Debemos pulsar sobre *Examinar*, e indicar la ubicación del archivo de certificado en nuestro equipo, cuando se haya seleccionado, únicamente queda hacer clic sobre Importar, y ya se habrá instalado el certificado.

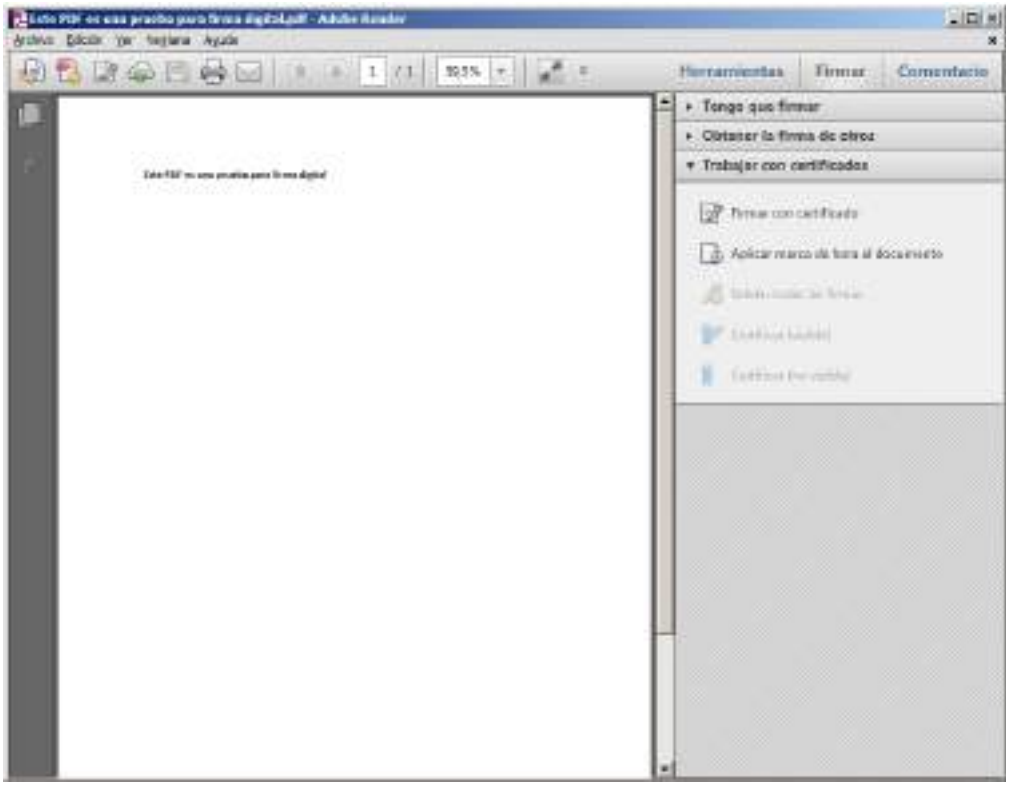
Es fundamental, ante todo de cara a validar firmas de documentos, que se realice una ajuste sobre la configuración del certificado instalado en el propio repositorio, para ello, en listado de autoridades de confianza, se debe seleccionar el certificado a editar (una vez instalado) y pulsar sobre el botón "*Editar confianza*", a lo que se accederá al siguiente panel.

Debemos asegurar que esté marcado el campo "*Utilizar este certificado como raíz de confianza*", en caso contrario, y aunque el certificado esté instalado, Adobe Reader seguirá dando por no válida una firma emitida por dicha Autoridad de Certificación. Una vez completados estos pasos, ya dispondríamos de nuestro certificado instalado en la aplicación y listo para firmar documentos.

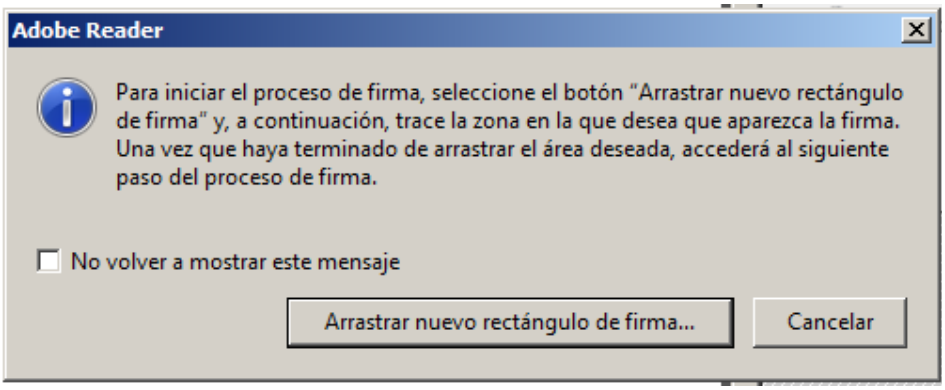
7.2. Firma de documentos

Para la realización de una **firma de un documento**, debemos de partir del estado de tener el documento que queremos firmar abierto con la herramienta Adobe Reader, una vez abierto debemos acceder al panel denominado *Firmar*, y dentro del mismo al apartado "*Trabajar con*

certificados".



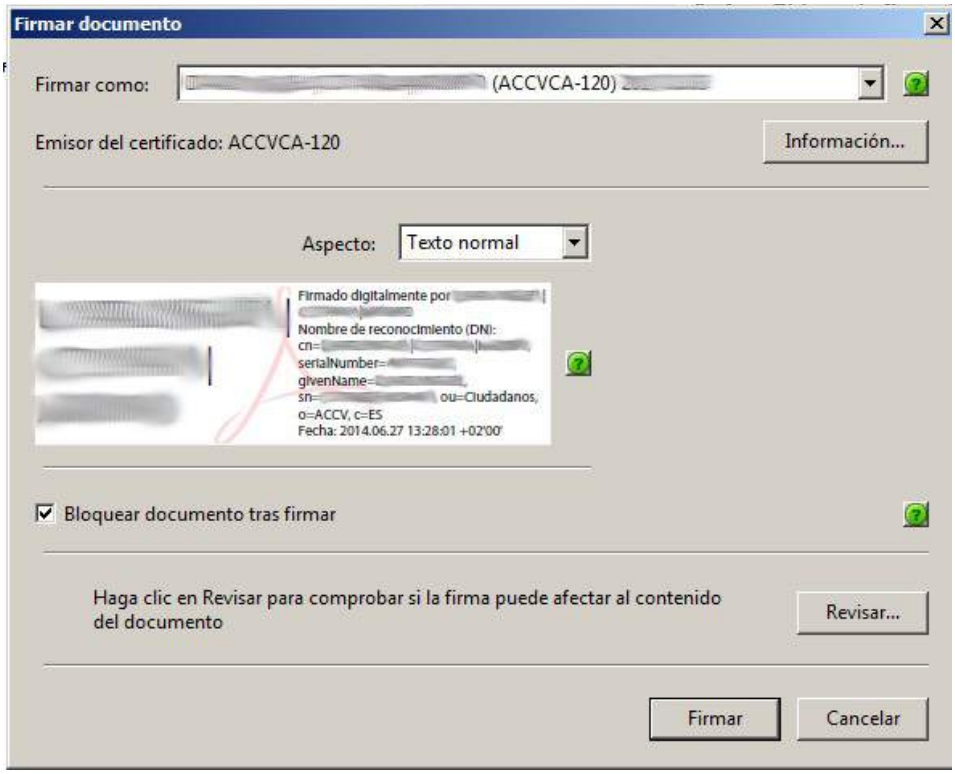
Para comenzar con el proceso de firma, debemos pulsar el botón "*Firmar con certificado*". A lo que se nos mostrará el siguiente diálogo:



Debemos seleccionar el botón "*Arrastrar nuevo rectángulo de firma*", y nos dejará con el documento que se desea firmar; el fin es seleccionar un área en la que aparecerán los datos de la firma digital, por lo que se

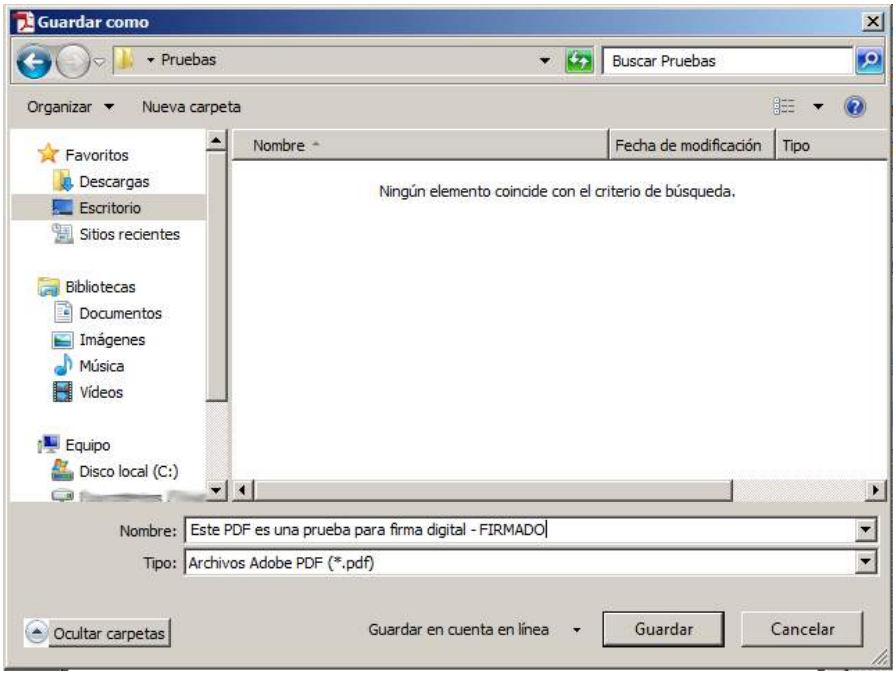
recomienda aprovechar alguna parte en blanco del documento, donde no exista texto.

Una vez seleccionada el área, se abrirá el dialogo siguiente:

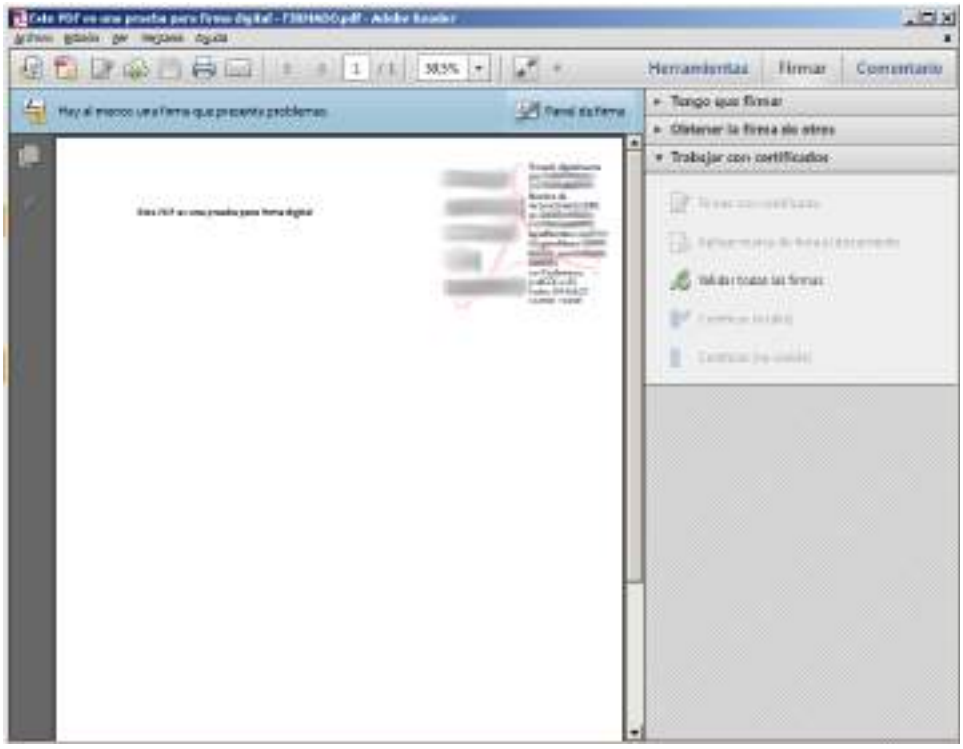


En este cuadro deberemos seleccionar el certificado con el que queremos firmar el documento, y se nos muestra una vista previa del recuadro de firma del documento. Es fundamental marcar "*Bloquear el documento tras firmar*", ya que así no se permitirá la edición del mismo tras la firma, asegurando la integridad el mismo. En cualquier caso, si en algún momento el documento se editara, la firma perdería su validez.

Una vez tengamos todo el formulario relleno en base a nuestros criterios, procederemos a pulsar sobre el botón *Firmar*.



Adobe Reader nos solicitará una ruta para guardar el documento pdf firmado, se selecciona y se pulsa en *Aceptar*. Y por fin tenemos nuestro documento firmado, quedaría como sigue:



Dejamos adicionalmente un enlace a vuestra disposición con las instrucciones facilitadas por el propio desarrollador del software para implementar firma.

7.3. Validar firma de un documento

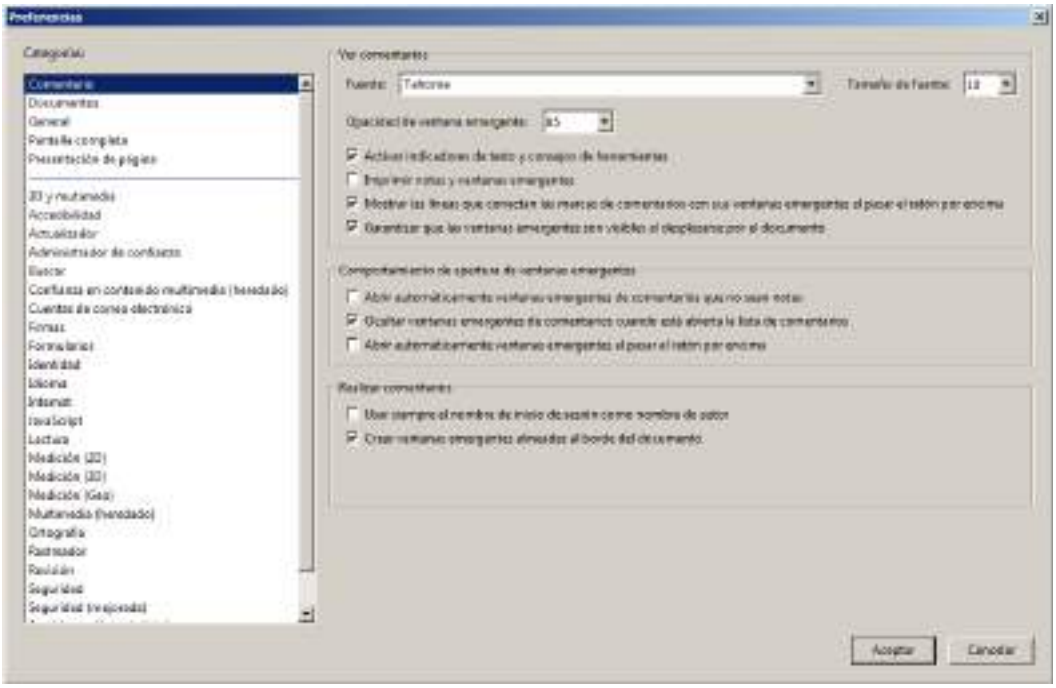
Tan importante es poder firmar documentos como poder **verificar las firmas de terceros**. En este consejo os enseñamos a configurar Adobe Reader para que realice una validación adecuada de firma digital. De este modo evitaréis dar como válida una firma digital que pueda haberse vulnerado o ser fraudulenta.

Para ilustrar el ejemplo, emplearemos el mismo documento que se implementó en el punto precedente, de modo que se compruebe la validez y confiabilidad de la firma implementada. El primer paso será pues, asegurar que la configuración de Adobe Reader es correcta.

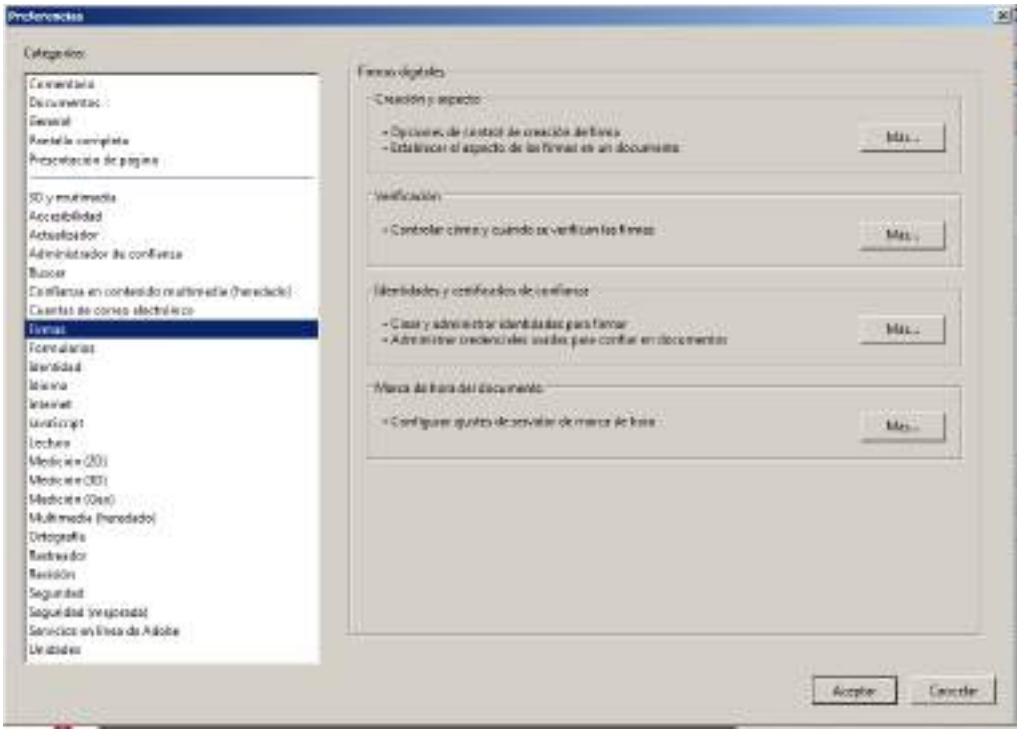
7.3.1. Configuración de validación de firma en Adobe Reader

En el presente punto se plantea una **configuración de la validación de firma digital** de documentos pdf con Adobe Reader. Se detallan los pasos a seguir a continuación.

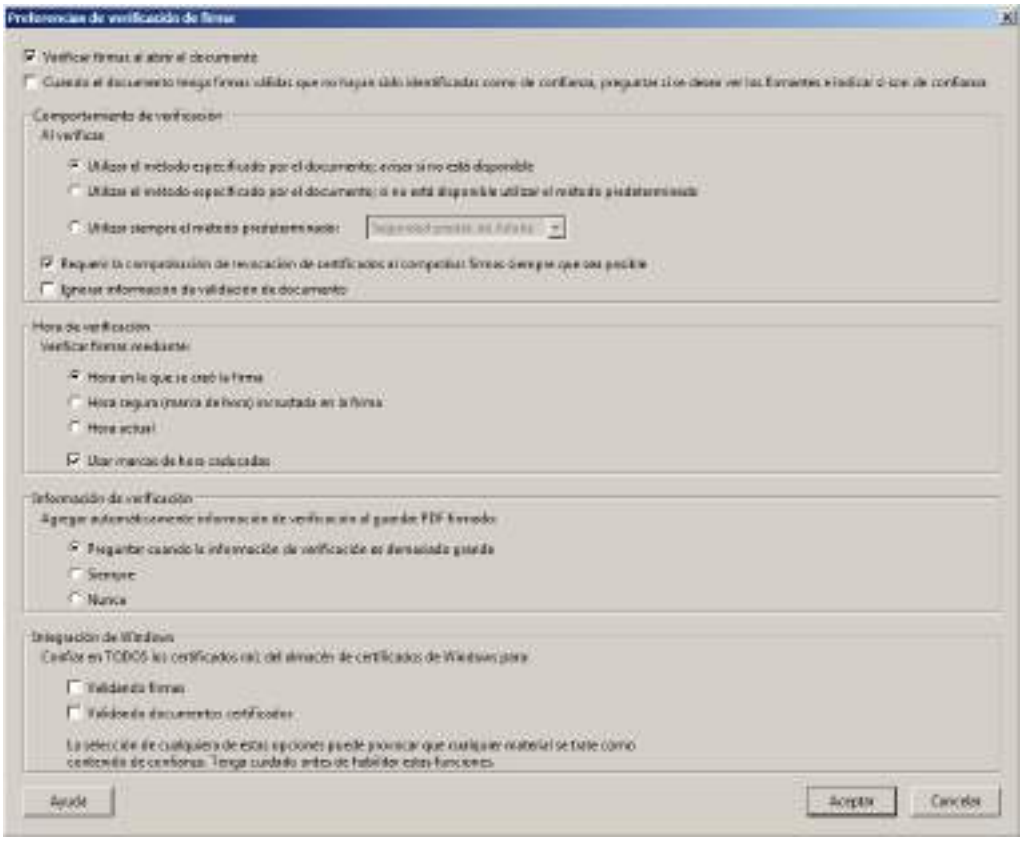
En primer lugar se debe acceder al panel preferencias, para ello se debe ir a *Edición* → *Preferencias*, debemos acceder a la ventana que se muestra a continuación:



A continuación debemos acceder al menú de *Firmas*. Mostrando las siguientes opciones:



Debemos acceder al menú de *Verificación*, en el mismo se muestran una serie de opciones que permiten configurar los parámetros relacionados con la validación de firmas de documentos. Se muestran los valores recomendados en la siguiente captura de pantalla.



Se detallan brevemente las opciones de configuración:

- *Verificar firmas al abrir el documento*: Fundamental, si no se marca no se realizará ninguna comprobación de la firma.
- *Cuando el documento tenga...*: No se recomienda su habilitación, ya que puede llevar al usuario a tomar decisiones sobre validez de certificados que pueden dar lugar a error. En caso de que un certificado de errores se recomienda referir a la Autoridad de Certificación emisora e instalar manualmente los certificados raíz de la misma como se detalla en el punto 7.1 de la presente guía.
- *Comportamiento de Verificación*: En este campo, se debe fijar que se intente validar la firma con el método especificado en el documento,

que depende directamente del certificado con el que se haya firmado, en caso de que no esté disponible avisará al usuario.

- *Hora de verificación*: Dado que un documento firmado digitalmente tendrá validez dependiendo de cuando se haya implementado la firma, dicha validación se debe realizar empleando la fecha en la que la firma se implementó, independientemente de si el certificado ha caducado a fecha de revisión del documento.
- *Información de verificación*: El software almacena información de la validación con el documento, de este modo se realizan las comprobaciones pertinentes cuando se valida el documento. Este valor es útil de cara a la firma de documentos, y no de para validar la firma de documentos recibidos. Se recomienda incluir la información para facilitar la validación por parte de terceros.
- *Integración con Windows*: Refiere a si Adobe Reader debe aceptar como legítimos los certificados de entidad instalados en el repositorio del sistema operativo Windows. Se recomienda que no sea así, y que se instalen los certificados recomendados por Adobe, así como que se instalen los certificados que se consideren de confianza manualmente.

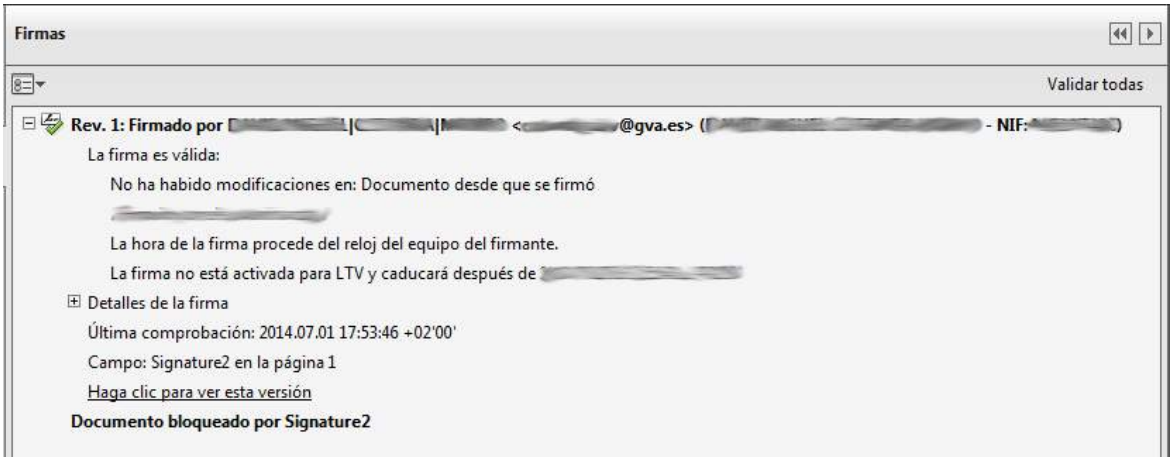
7.3.2. Verificación del documento

Una vez configurada adecuadamente la aplicación, y cuando procedemos a abrir un documento firmado digitalmente, se nos mostrará un mensaje en la parte superior del documento que nos dará una idea sobre el estado general de la firma del documento. Pueden darse los siguientes casos:

- En caso de que la firma sea válida

- En caso de que se identifique algún problema con la misma

En cualquier caso, y ante todo en el caso de que se **identifique algún problema con la firma**, se debe acceder al *Panel de firma* pulsando sobre el botón. Se despliega un menú en el que se muestran las comprobaciones realizadas sobre la firma, así como el resultado de las mismas, se muestra un ejemplo a continuación:



Como se puede observar, **se detalla en lenguaje natural cualquier tipo de problema que pueda haberse declarado en la firma**, así como las condiciones de la marca de tiempo o hora de la firma (marca que se incluye en la firma digital para detallar la fecha y hora en la que se firmó el documento).

En caso de que se produzca cualquier problema, se recomienda **ponerse en contacto con el remitente o firmante del documento empleando un medio alternativo al de la recepción del documento**, y en su caso, con la Autoridad de Certificación responsable del certificado. Esta información se puede obtener de la información de la firma, a la que se puede acceder desde el panel de firmas, pulsando con el clic derecho sobre la firma que da problemas y accediendo a "*Propiedades de la firma*" → "*Mostrar certificado de firmante*" y revisando los campos Sujeto para el firmante, y emisor para la Autoridad de certificación.

Dejamos un enlace con más información sobre configuración y validación

de firmas con Adobe Reader.

8. Resumen y conclusiones

Como se ha ido detallando a lo largo de toda esta guía, l**os certificados digitales tienen un uso muy extendido en internet**, dado que se emplean para autenticar la gran mayoría de identidades y sitios en la red, así como para cifrar la mayoría de las comunicaciones. Son un **mecanismo muy potente, y muy seguro**; pero como suele pasar en la gran mayoría de los casos con cualquier mecanismo, por seguro que sea, **si se hace un uso negligente del mismo entraña muchos más riesgos que beneficios**.

Desde CSIRT-cv esperamos que esta guía ayude a los ciudadanos a poder emplear este mecanismo de una forma segura, conociendo todos los riesgos de su uso pero desde una **óptica de confianza**. **El conocimiento de los riesgos no debe asustar, sino aportar seguridad a la hora de aprovechar todas las ventajas y servicios que nos puede dar la sociedad de la información**.

Por último, agradecer vuestra atención y recordar que desde CSIRT-cv prestamos servicio a toda la Comunidad Valenciana, por lo que, en caso de que pueda surgir cualquier duda sobre el contenido de esta guía o cualquier problema de seguridad, así como si identificáis cualquier errata en el presente documento podéis poneros en contacto con nosotros bien a través de nuestro portal web (http://www.csirtcv.gva.es/) o a través de correo electrónico a la cuenta csirtcv@gva.es.

9. ANEXO - Certificados de Ciudadano y Empleado Público de la Agencia de Tecnología y Certificación de la Comunidad Valenciana (ACCV)

La **Agencia de Tecnología y Certificación Electrónica** (en adelante ACCV) es un departamento del Instituto Valenciano de Finanzas, a través de que se proporciona a los ciudadanos, las empresas y las Administraciones Públicas los mecanismos de identificación telemática segura en los trámites administrativos a través de Internet: los certificados digitales y las tecnologías asociadas.

Los certificados emitidos y el resto de servicios que la ACCV presta se ajustan a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, por lo que la **ACCV goza de amplio reconocimiento en todas las Administraciones Públicas**. Además, con los certificados digitales reconocidos expedidos por la ACCV se puede generar **firma electrónica reconocida**, que es equivalente a la manuscrita.

La ACCV se plantea los siguientes objetivos:

- Ofrecer a los ciudadanos, las empresas, las Administraciones Públicas, las Universidades y los Colegios Profesionales los **instrumentos necesarios para garantizar la seguridad y la validez legal de las transacciones telemáticas**.
- Fomentar y contribuir al **desarrollo de aplicaciones y servicios telemáticos**, en beneficio de los ciudadanos, las empresas y las Administraciones. Para la consecución de este objetivo es crucial la coordinación y la interoperabilidad técnica entre Administraciones y con otros Prestadores de Servicios de Certificación.

- Potenciar la **formación de ciudadanos y empleados públicos** a través de acciones formativas específicas (cursos impartidos a través del Instituto Valenciano de Administraciones Públicas y en el Centro Virtual de Formación al Ciudadano).
- Proveer del **soporte necesario en el uso de las nuevas tecnologías**, con el fin de conseguir el desarrollo de una **cultura digital** que facilite el **desarrollo de la Sociedad de la Información en la Comunidad Valenciana**.
- Promover la **colaboración técnica** y el reconocimiento mutuo entre la ACCV y otros Prestadores de Servicios de Certificación con miras a la **universalización del uso de los certificados**.

El objetivo del presente anexo es facilitar al lector información para la **obtención y gestión de certificados digitales de ACCV**. Una vez presentado el centro y dicho lo propio, se pasa a las recomendaciones en sí mismas.

NOTA IMPORTANTE: El contenido detallado en esta sección se ha extraído en su gran mayoría de la página web de ACCV, por lo que se remite a la misma para ampliar cualquier información de interés que no pueda estar incluida en esta guía.

9.1. Consideraciones generales

9.1.1. Puntos de Registro de Usuario

Los Ciudadanos que deseen solicitar un certificado digital deben dirigirse a cualquiera de los **Puntos de Registro de Usuario (PRU)** que existen en la Comunidad Valenciana.

La solicitud del certificado digital es presencial y el solicitante deberá

identificarse mediante su D.N.I, N.I.E o pasaporte español, en vigor (debe aportar original y fotocopia).

Más información, así como un mapa interactivo para encontrar el punto de registro de usuario más cercano en cualquiera de las siguientes URL.

Ciudadanos - http://www.accv.es/ciudadanos/puntos-de-registro-de-usuario/

Empleados públicos - http://www.accv.es/administracion-publica/puntos-de-registro-de-usuario/

9.1.2. Área Personal de Servicios de Certificación (APSC)

El **Área Personal de Servicios de Certificación (APSC)** es una aplicación web que permite la gestión de los certificados reconocidos de ciudadano, de empleado público y de pertenencia a empresa emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV), a través de Internet y de forma segura.

El acceso a APSC **requiere un certificado reconocido de ciudadano**, de empleado público o de pertenencia a empresa emitido por la ACCV. **También puede acceder con DNI electrónico** para solicitar un certificado reconocido de ciudadano en soporte software.

Los **servicios disponibles** a través del APSC son los siguientes:

- Consulta del estado y los datos del certificado.
- Rectificación de los datos personales.
- Renovar los certificados.

- Revocar los certificados.
- Descargar el fichero seguro cifrado (para certificados reconocidos de ciudadano).
- Obtención del certificado reconocido de ciudadano en soporte software (si dispone de un certificado en tarjeta criptográfica, de ciudadano, de empleado público o de pertenencia a empresa, o del DNI Electrónico).

Para acceder a ASPC se requiere un certificado vigente de ACCV instalado en el navegador. Se puede acceder a la misma en el siguiente enlace de acceso.

9.1.3. Soporte

En primer lugar, ACCV pone a disposición de los usuarios un apartado de ayuda en su sitio web en el que se puede encontrar información y respuesta a dudas frecuentes respecto a sus certificados, podéis acceder aquí.

Para el contenido que no esté incluido en el apartado de Ayuda, ACCV mantiene, medios para la consulta directa con su personal. Se pueden realizar sus consultas a través del teléfono de soporte **902 482 481** o a través del **Formulario de Atención al Usuario**.

9.2. Certificados de Ciudadano en Soporte Software

Los **Certificados Reconocidos de Ciudadano en Soporte Software** emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV) se proporcionan en el navegador web y en soporte fichero (extensión .p12).

9.2.1. Uso

Los certificados reconocidos de ciudadano emitidos por la ACCV se pueden utilizar para:

- **Firmar y cifrar** de forma segura cualquier tipo de documento electrónico incluidos los mensajes de correo electrónico.
- La **identificación de usuarios** ante servicios telemáticos de la Administración Pública y las entidades privadas.

9.2.2. Como solicitar un certificado

La emisión de los certificados reconocidos de ciudadano en soporte software se realiza de **forma telemática** con una **solicitud previa presencial en un Punto de Registro de Usuario de la ACCV** (PRU), en la que se procede a la identificación del solicitante.

Los pasos a seguir son:

- Acudir a cualquiera de los Puntos de Registro de Usuario (PRU) que existen en la Comunidad Valenciana e identificarse con su **DNI, NIE o pasaporte español válido**.

  Tras realizar su identificación el operador le facilitará el **Código de Generación de Certificados**.
- Acceder al **Frontal de Generación de Certificados Digitales** de la Agencia de Tecnología y Certificación Electrónica para completar la emisión del certificado digital. Podéis encontrarlo en la siguiente URL.

Cuando ya se ha obtenido Código de Generación del certificado digital en el PRU correspondiente, se dispone de dos alternativas para generar su **certificado digital de firma**.

En ambos casos deberá acceder al **Frontal de Generación de Certificados Digitales** e introducir su DNI/NIE y el Código que le han

facilitado en el PRU.

- **Directamente en el navegador web que vaya a utilizar:**

  El certificado queda instalado durante la generación y no es necesaria instalación posterior.

  Durante el proceso definirá una **contraseña del navegador** que lo protege y deberá introducir cuando vaya a operar con el certificado.

  Por seguridad recomendamos **exportar el certificado a un fichero .p12** para posteriores instalaciones en otros navegadores u ordenadores. Más información al respecto en el portal de ACCV en el siguiente enlace.

- **En un fichero .p12:**

  Una vez obtenido deberá instalarlo en el navegador siguiendo los pasos de las guías de instalación.

  Durante el proceso definirá una **contraseña del fichero** que deberá introducir para realizar su instalación en el navegador.

  Para instalar el certificado en el navegador se pueden seguir las directivas establecidas en la presente guía en el apartado 3.1 – Identificación Digital o en las guías que mantiene ACCV a tal efecto en el siguiente enlace.

9.2.3. Código de generación de certificados

La propia ACCV facilita la siguiente información sobre el uso del **código de generación de certificados**, que se requiere para la generación de certificados de ciudadano en Soporte Software:

- El código tiene 25 caracteres y distingue mayúsculas y minúsculas. Introduzca con cuidado cada uno de los caracteres en el campo del formulario web destinado al mismo ya que para la correcta generación debe ser exactamente el facilitado en el Punto de Registro de Usuario (PRU). Si se introduce tres veces mal se bloquea indefinidamente, por

lo que se deberá solicitar uno nuevo en el PRU.

- Se dispone de un plazo de dos semanas desde la obtención del código en el PRU para completar la generación a través de la página web de la ACCV. En caso contrario caduca y deberá solicitar uno nuevo en el PRU.
- A través del código cualquier persona que pudiera conocer además el DNI/NIE del beneficiario del certificado podría suplantarle y obtener el certificado digital en su lugar. Por motivos de seguridad en este caso ACCV ruega que se mantenga el código bajo custodia y en ningún caso lo conserve junto al DNI/NIE.

9.2.4. Obtención de certificados de cifrado

Una vez obtenido e instalado el certificado digital en el navegador web, únicamente será necesario acceder al Área Personal de Servicios de Certificación (ASPC) para descargar el archivo .p12 correspondiente al certificado de cifrado. Se muestra a continuación una captura de pantalla de la página principal del ASPC.

Debemos hacer clic sobre "*Ficheros de Cifrado*", en la barra de menú superior, accediendo a un listado de los certificados de cifrado disponibles, su fecha de emisión y su estado.

Para descargar el fichero de cifrado, únicamente debemos seleccionar el deseado mediante la opción *Descargar*, y automáticamente comenzará su descarga en el navegador.

Una vez descargado el fichero, se mostrará en la página web la opción "*Ver PIN*", se debe hacer clic y anotar en una ubicación segura dicho PIN, que nos permitirá instalar la clave de cifrado donde deseemos.

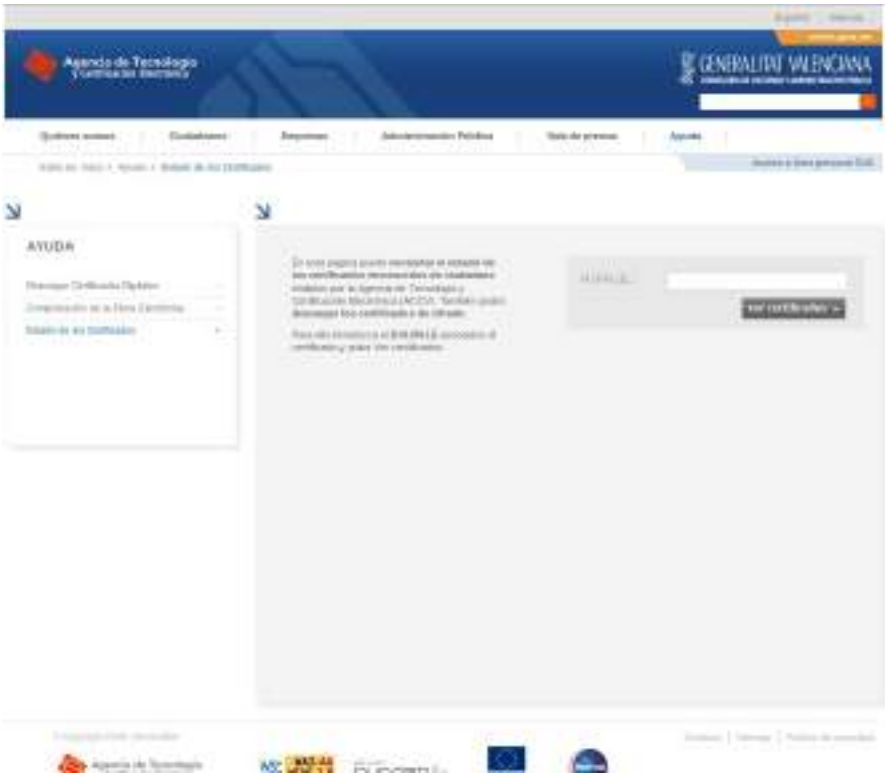
Para instalar la clave de cifrado, por ejemplo para descifrar correo electrónico, se han facilitado instrucciones en la presente guía, concretamente en el punto 4.Uso de Certificados Digitales en Correo Electrónico; adicionalmente la ACCV mantiene instrucciones adicionales en el siguiente

enlace.

Una vez disponemos de la clave instalada en nuestro cliente de correo, es fundamental tener en cuenta que la persona que desee cifrar correo para nosotros debe disponer de la clave pública de nuestro certificado, que no es la misma que la del certificado de firma (son dos certificados distintos); para ello, el método más sencillo es que la descargue mediante la página de Consulta de Estado de Certificados de Ciudadano, para ello únicamente necesita conocer el DNI/NIE de la persona a la que quiere cifrar el correo, que lo puede obtener fácilmente de un correo firmado digitalmente.

La interfaz web nos solicita el DNI del propietario de los certificados que deseamos consultar. Una vez realizada la consulta, y en el caso de que el identificador esté registrado, se listarán todos los certificados digitales que han pertenecido a dicha persona, apareciendo siempre en la parte superior los que puedan ser vigentes.

Se puede descargar la clave pública del certificado de cifrado pulsando *Descargar* en el sitio web, y posteriormente instalándolo en el repositorio de certificados correspondiente a nuestro cliente de correo, como se detalla en el punto 4.Uso de Certificados Digitales en Correo Electrónico. Se muestran capturas de pantalla de referencia a continuación.



9.2.5. Renovación

Los **certificados reconocidos de ciudadano** emitidos por la

Autoridad de Certificación de la Comunidad Valenciana (ACCV) tienen un **periodo de validez de tres años**. ACCV pone a disposición de los cualquiera un servicio para comprobar la **fecha de caducidad** de cualquier certificado emitido por la Agencia a través del enlace Comprobar el estado de los certificados digitales.

Cuando un certificado digital vaya a caducar la ACCV informará a la persona afectada a través de un correo electrónico. Durante el **periodo de renovación de su certificado digital** se puede solicitar un nuevo certificado digital, en el mismo soporte que el anterior, a través del Área Personal de Servicios de Certificación. El periodo de renovación se inicia **70 días antes de la fecha de caducidad** (cuando el usuario recibe el correo) y termina en la propia fecha de caducidad.

Adicionalmente y en cualquier momento, se puede solicitar la renovación del certificado acudiendo a un **Punto de Registro de Usuario** (PRU) e identificándose con su **D.N.I., N.I.E. o pasaporte español en vigor**.

9.2.6. Revocación

Revocación a través del Área Personal de Servicios de Certificación

Se puede solicitar la revocación de un certificado digital a través del Área Personal de Servicios de Certificación.

Desde esta aplicación web se envía a la ACCV una solicitud remota de revocación de certificados de usuario (Certificados Reconocidos en Soporte Software para Ciudadanos o Certificados Reconocidos en Dispositivo Seguro para Ciudadanos).

Revocación Telefónica

Para realizar una solicitud de revocación telefónica se puede llamar al

teléfono de Soporte de la Autoridad de Certificación de la Comunidad Valenciana (902 482 481) y solicitar la revocación de los certificados.

Los Operadores comprueban la identidad del usuario preguntándole sus datos personales. En este instante, el certificado del usuario queda Suspendido hasta que la Autoridad de Certificación contacta con el usuario para confirmar la identidad y verificar el procedimiento de Revocación.

Una vez que se suspende el certificado, el usuario propietario del mismo recibe un correo electrónico en la cuenta asociada al certificado notificándole el cambio de estado del mismo. La revocación posterior se notifica al usuario de la misma forma.

Revocación presencial

El último de los medios es completamente presencial, para ello se puede acudir a un Punto de Registro e identificarse con su D.N.I, N.I.E o Pasaporte Español, en vigor. Se debe solicitar la Revocación de su Certificado al Operador del Punto de Registro e indicarle el motivo.

Una vez que se revoca el certificado, el usuario recibe un correo electrónico en la cuenta asociada al certificado notificándole el cambio de estado del mismo.

9.2.7. Ciudadano en Dispositivo Seguro

De cara a los ciudadanos que consideren que quieren disponer de su **certificado en un dispositivo criptográfico seguro**, ACCV también ofrece este servicio. Se detalla en que consiste el uso de un certificado en dispositivo seguro en el apartado de la guía 3.4.Certificados digitales en soporte hardware. Se remite en este caso al apartado correspondiente dentro del sitio web corporativo de la Agencia, en el que se puede encontrar información concreta de como puede obtenerse un certificado de este tipo.

9.3. Empleado Público

Los **certificados reconocidos de empleado público** emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV) se proporcionan en **tarjeta criptográfica** y están sujetos a las condiciones de uso, limitaciones y responsabilidades establecidas en la Política de Certificación de certificados reconocidos de empleado público.

Estos certificados tienen **una validez de tres años** y gozan de amplio reconocimiento por parte de las Administraciones Públicas españolas, por estar registrados por parte del **Ministerio de Industria, Turismo y Comercio** y por estar integrados en la **plataforma @firma**.

9.3.1. ¿Para qué se utilizan?

El grupo de usuarios que puede utilizar este tipo de certificado digital está formado por los **empleados públicos que trabajan para cualquier tipo de Administración Pública** (europea, estatal, autonómica y local) así como los empleados de sus entes instrumentales y los empleados de las Corporaciones y Universidades Públicas.

Los certificados reconocidos de empleado público emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV) sirven para identificar a los empleados de los organismos en el ejercicio de sus competencias. Como ejemplo a destacar, este tipo de certificado digital se utiliza para **el perfil del contratante de la Generalitat** o para **solicitar los certificados de Sede Electrónica y Sello de Órgano**.

9.3.2. ¿Quién los puede solicitar?

Los **responsables de las entidades** interesadas deben **contactar directamente con la ACCV** para formular la solicitud de certificados de

empleado público para su personal.

AVISO: Los empleados públicos no pueden solicitar a título personal y de forma autónoma este tipo de certificados. Serán los responsables de la entidad en la que desarrollan su actividad quienes formularán la solicitud a la ACCV.

9.3.3. ¿Cómo se solicitan?

Las entidades interesadas en la solicitud de certificados de empleado público para su personal deben completar el formulario siguiente y enviarlo a la ACCV (a gestioncerts@accv.es o al fax 961971771):

Formulario de alta de la organización

En él constan los responsables del organismo habilitados para la solicitud de certificados de empleado público. Estas personas se encargarán de **la solicitud de alta, entrega y revocación**. Además, se comprometen a informar a los usuarios de sus obligaciones y responsabilidades y a remitir los contratos de certificación firmados a la ACCV. El formulario se puede encontrar aquí.

El formulario de alta **debe cumplimentarse únicamente la primera vez** que el organismo vaya a solicitar certificados de empleado público o cuando haya **alguna modificación en los autorizados**.

Una vez recibida la solicitud en la ACCV verificaremos la información y les confirmaremos a través de un correo electrónico que la organización ha sido dada de alta.

Entorno de solicitud de certificados

En este Entorno de Gestión EP, se identificará mediante certificado a aquellos habilitados para llevar a cabo las gestiones relativas a los certificados

de empleado público. Una vez identificados, podrán cumplimentar un formulario de solicitud de certificados para empleados públicos pertenecientes a su Administración o, alternativamente, enviar un fichero con formato CSV para agilizar la remisión de los datos cuando son muchas las solicitudes. Se pone a disposición de los interesados en el siguiente enlace.

Para poder acceder a este entorno de solicitud de certificados de Empleado Público es imprescindible disponer de un certificado personal válido emitido por la Agencia de Tecnología y Certificación Electrónica y haber sido habilitado por la entidad o administración pública titular de los certificados (mediante la cumplimentación del alta de la entidad anteriormente descrita).

IMPORTANTE: Sólo en casos excepcionales y justificados se aceptarán solicitudes de certificados de Empleado Público por canales o medios diferentes al Entorno de Gestión EP.

9.4. ¿Qué se entrega al solicitante?

Cuando la emisión se haya completado, la ACCV enviará al responsable del organismo las tarjetas criptográficas que contienen los certificados digitales y su PIN/PUK (en sobre ciego o rotagrama).

9.5. Renovación

La renovación de los certificados de empleado público la debe realizar el titular del certificado a través del **Área Personal de Servicios de Certificación (APSC)**.

Con carácter previo es necesario que los responsables de las entidades interesadas en renovar los certificados soliciten a la ACCV un presupuesto (por correo electrónico a la cuenta gestioncerts@accv.es o a través del fax

961971771), detallando **el número de certificados a renovar**.

Una vez aprobado el presupuesto por la entidad, la ACCV le autorizará para la renovación del número de certificados solicitado.

Cada titular de certificado de empleado público recibirá un correo informativo de la ACCV cuando el certificado vaya a caducar. A partir de ese momento podrá solicitar un nuevo certificado digital a través del Área Personal de Servicios de Certificación (APSC). Para ello debe estar **autorizado por su entidad u organismo** (en caso contrario la aplicación le mostrará un mensaje de aviso y deberá contactar con el responsable de la entidad), tal y como se describe en este apartado.

AVISO: Para renovar el certificado a través de APSC éste debe ser válido y estar en periodo de renovación (dentro de los 70 días anteriores a su caducidad).

En caso de que tenga cualquier duda sobre la caducidad del certificado digital a su disposición, puede comprobar su estado fácilmente en el siguiente enlace.

9.6. Revocación

Si el titular de un certificado de empleado público desea revocarlo debe dirigirse al responsable habilitado para la solicitud y gestión de los certificados de empleado público en su organización, quien deberá completar el formulario a continuación y remitirlo a la ACCV (a gestioncerts@accv.es o al fax 961971771). Se puede obtener el formulario en el siguiente enlace.

AVISO: Si el titular de un certificado reconocido de empleado público cesa en su cargo o cambia de puesto, el certificado deja de ser vigente y debe ser

revocado. Por este motivo **ES MUY IMPORTANTE** solicitar la revocación de dicho certificado digital.

Esta solicitud de revocación puede llevarla a cabo cualquier persona que conozca la situación, no siendo necesario que se persone el titular. En ese caso desde la ACCV se harán las comprobaciones necesarias antes de la revocación.

Posteriormente la solicitud del certificado para el nuevo titular debe llevarse a cabo según el procedimiento habitual descrito en apartados anteriores.