

SUITE CRITICAL ACCESS®

ANF AUTORIDAD DE CERTIFICACIÓN

GUÍA DE USUARIO

Versión 2.0



OID 1.3.6.1.4.1.18332.6.1



Edición:

IBD, S.A

Depósito Legal N°:

B-8-3800-2010

ISBN N°:

978-84-613-7461-8

Nivel de Seguridad

Documento Público

Aprobado Junta Rectora PKI ANF AC

Fecha de Creación 20 de Febrero 2019

OID 1.3.6.1.4.1.18332.6.1

**Este documento es propiedad de ANF Autoridad de Certificación.
Se autoriza su reproducción y difusión siempre que se reseñe:**

2019 Copyright © ANF Autoridad de Certificación.

ÍNDICE

1. Gestión de certificados	
1.1 Puesta a punto de su certificado	04
• Abrir Suite Critical Access	06
• Activar la solicitud	07
• Descargar	10
• Exportar	12
1.2. Cambiar PIN	17
1.3. Ver el Localizador y otros datos del certificado	18
1.4. Renovar certificado	20
1.5. Revocar	21
2. Firma electrónica	22
2.1. Firmar electrónicamente un documento PDF (PAdES)	23
2.2. Firmar electrónicamente un archivo XML (XAdES)	25
2.3. Firmar electrónicamente cualquier otro archivo (CAAdES)	25
3. Validación de firmas electrónicas, certificados y sellos de tiempo	26
3.1. Validación Cualificada	27
3.2. Validación Avanzada	28
3.3. Certificado	29
3.4. Sello de tiempo	30
4. Actualización del Critical	31

1. GESTIÓN DE CERTIFICADOS

1.1 PUESTA A PUNTO DE SU CERTIFICADO

Tras finalizar la solicitud de su certificado frente a una Autoridad de Registro u Oficina de Verificación Presencial de ANF AC, habrá recibido un dispositivo eSign (*Token*), con su solicitud pendiente de ser activada. A la vez, usted habrá recibido 2 contraseñas de activación, una al correo electrónico y otra por SMS.



Dispositivo eSign (*token*)



Contraseña correo electrónico

* * * *

Contraseña SMS

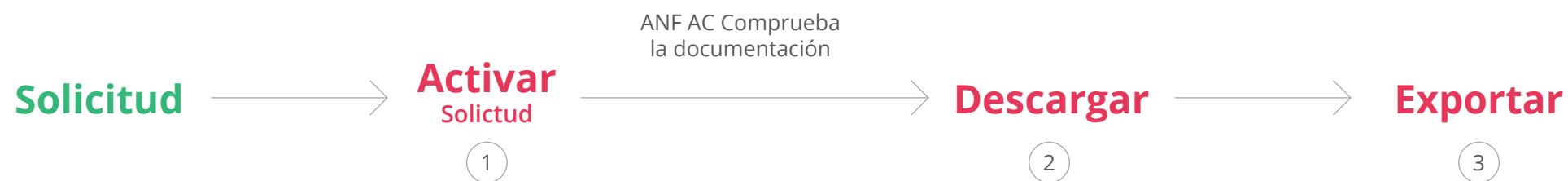
* * * *

1. GESTIÓN DE CERTIFICADOS

1.1 PUESTA A PUNTO DE SU CERTIFICADO

Una vez haya activado su solicitud, ANF AC la recibirá y procederá a la comprobación de la documentación. Si todo es correcto, recibirá un correo electrónico de confirmación y su certificado será emitido. **Este proceso puede demorar un tiempo estimado de 24 a 48h.**

Entonces, podrá proceder a realizar los procesos de **descarga** y **exportación**, desde el mismo programa.



Siga con atención los pasos de esta Guía para poner a punto su certificado electrónico.

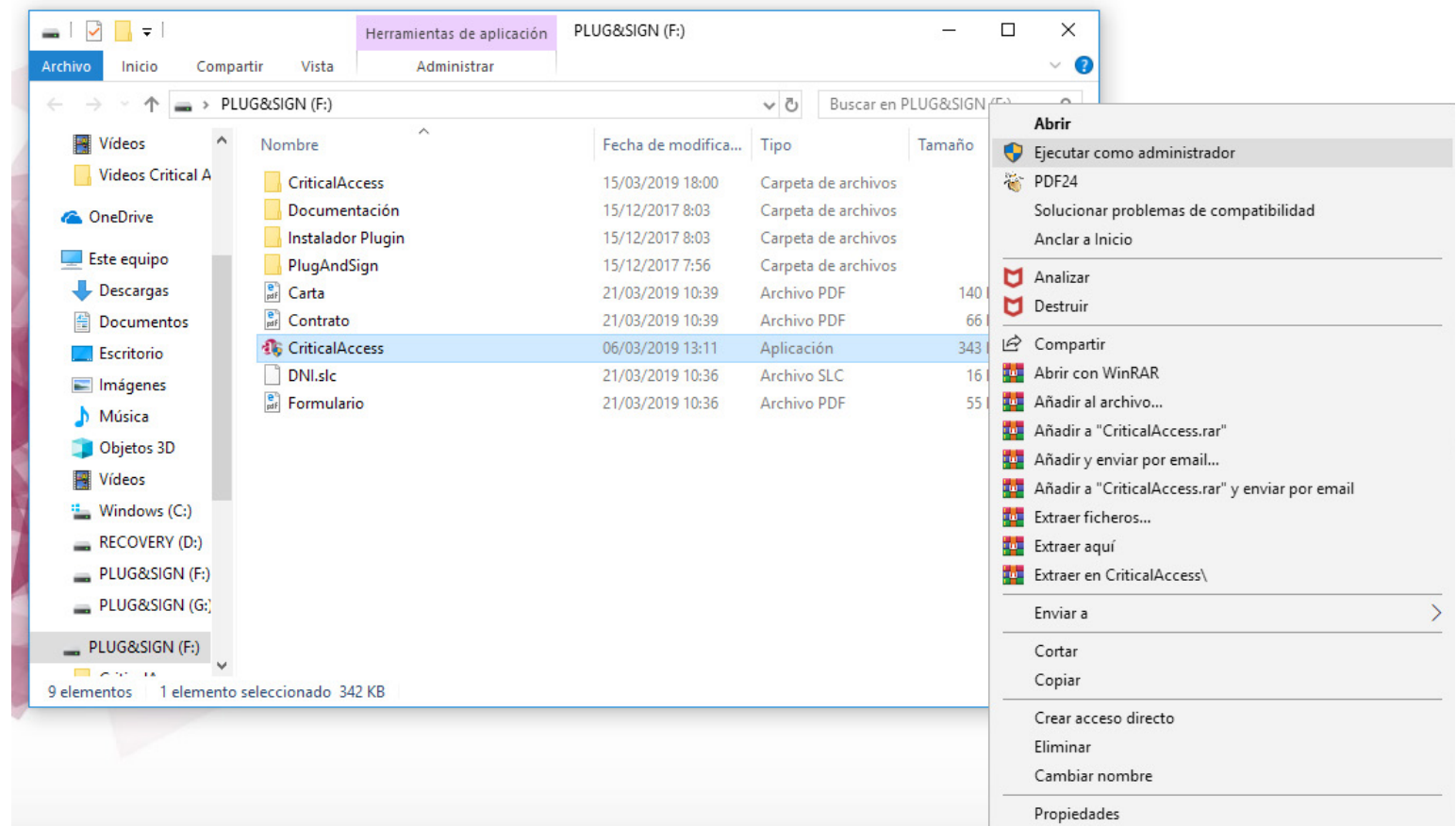
1. GESTIÓN DE CERTIFICADOS

• ABRIR SUITE CRITICAL ACCESS

Conecte su dispositivo eSign al ordenador. Dentro, encontrará el programa Suite Critical Access. Pulse sobre el botón derecho y "Ejecutar como administrador".

Usted puede obtener la versión más reciente del Critical Access a través de nuestra página web <https://anf.es/es/inicio> en el apartado "catalogo" y descargar el archivo comprimido.

Una vez descargado, debe descomprimir la carpeta en el disco C de su ordenador y ejecutar o abrir el archivo en .exe, del tipo aplicación, que se encuentra en la carpeta.



1. GESTIÓN DE CERTIFICADOS

• ACTIVAR SOLICITUD

Para realizar la activación de la solicitud, en la Suite Critical Access pulse sobre > Firma electrónica > Certificado electrónico > Activar

Posteriormente:

1. Seleccionar su dispositivo eSign donde activar el certificado y el localizador de la solicitud a activar. Presione activar.
2. Deberá establecer un PIN de seguridad por cada tipo de certificado, que deberá volver a introducir cuando descargue su certificado en los pasos siguientes. Además, deberá introducir un PUK, en caso de olvido del PIN.
3. Su solicitud ya se encuentra activada, cualquier error o inconveniente puede consultar en la lista de preguntas frecuentes de la web de ANF AC <https://www.anf.es/centro-de-ayuda/>.
4. La solicitud de su certificado está pendiente de ser validada y de emitirse. Este proceso puede demorar de 24 a 48h. Puede comprobar el estado de su certificado de la siguiente manera:

Certificado electrónico - Activar

1. Seleccione el dispositivo donde desea activar el certificado

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	
Plug and sign	G:\	PLUG&SIGN (G:)	4.0 GB	

2. Seleccione el localizador de la solicitud a activar

133012572-130075795

3. Introduzca las contraseñas de activación

Contraseña carta

Contraseña email

1. GESTIÓN DE CERTIFICADOS

• ACTIVAR SOLICITUD

1. Ir a Firma electrónica > Certificado electrónico > Consultar
2. Seleccionar el token correspondiente (*donde se encuentra el certificado*) y el certificado.

Para consultar el estado de validación de su certificado:

3. Presionar el botón “Ver validez”

De esta manera podrá conocer si el certificado ya se encuentra en nuestros servidores.

📄
Certificado Electrónico - Consultar

Dispositivos Conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and Sign	E:\	PLUG&SIGN (I)	4.0 GB	🔌
WINDOWS	WINDOWS			🔌

Relación de certificados almacenados en el dispositivo seleccionado

Datos Certificado
CERTIFICADO DE PERSONA FÍSICA - NOMBRE APELLIDO APELLIDO (AUTENTICACIÓN)
CERTIFICADO DE PERSONA FÍSICA - NOMBRE APELLIDO APELLIDO (FIRMA)
CERTIFICADO DE PERSONA FÍSICA - NOMBRE APELLIDO APELLIDO (CIFRADO)

←

Estos certificados **en rojo** están pendientes de Validar y de Emitir - (Debe esperar 24 - 48h)

Anterior

Ver Validez

Ver detalles

1. GESTIÓN DE CERTIFICADOS

• ACTIVAR SOLICITUD

Para consultar el estado de emisión de su certificado:

4. Si su certificado se encuentra emitido aparece el botón "descargar" en letras azules a la derecha de las letras rojas que identifican el certificado.

Certificado Electrónico · Consultar

Dispositivos Conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and Sign	I:\	PLUG&SIGN (!)	4.0 GB	
WINDOWS	WINDOWS			

Relación de certificados almacenados en el dispositivo seleccionado

Datos Certificado	
CERTIFICADO DE PERSONA FÍSICA -NOMBRE APELLIDO APELLIDO (AUTENTICACIÓN)	Descargar
CERTIFICADO DE PERSONA FÍSICA -NOMBRE APELLIDO APELLIDO (FIRMA)	Descargar
CERTIFICADO DE PERSONA FÍSICA -NOMBRE APELLIDO APELLIDO (CIFRADO)	Descargar

Certificados en negro + botón de descargar:
Ya han sido validados y emitidos, debe descargar

Anterior Ver Validez Ver detalles

1. GESTIÓN DE CERTIFICADOS

• DESCARGAR

1. Ir a Firma electrónica > Certificado electrónico > Consultar
2. Seleccionar el token correspondiente (*donde se encuentra el certificado*) y se despliega una lista de certificados en el recuadro de abajo.
3. Hacer clic sobre “descargar” (*letras azules que se encuentran a la derecha de cada certificado*). Deberá introducir el PIN que ha establecido en el paso de Activación.

The screenshot shows the 'Certificado electrónico - Consultar' interface. At the top, there is a header with the application logo and navigation icons. Below the header, a green bar contains the title 'Certificado electrónico - Consultar'. The main content area is divided into two sections:

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	
Windows	Windows			

Relación de certificados almacenados en el dispositivo seleccionado

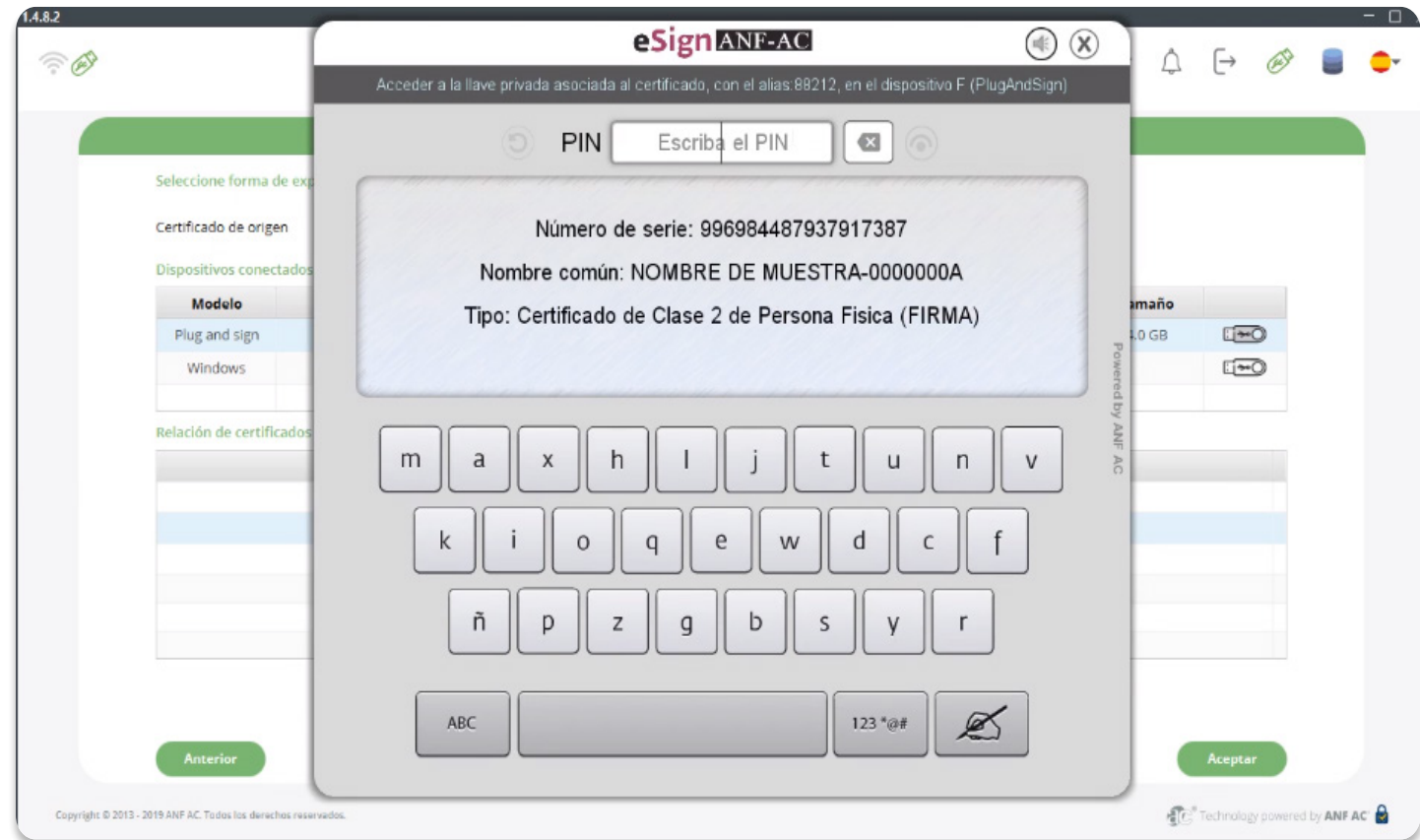
Datos certificado		
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (CIFRADO)		Descargar
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (FIRMA)		Descargar
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (AUTENTICACION)		Descargar

At the bottom of the interface, there are three buttons: 'Anterior', 'Ver validez', and 'Ver detalles'. The footer contains the copyright information: 'Copyright © 2013 - 2019 ANF AC. Todos los derechos reservados.' and the logo 'Technology powered by ANF AC'.

1. GESTIÓN DE CERTIFICADOS

• DESCARGAR

4. Escribir el PIN establecido al momento de la Activación de la solicitud.



1. GESTIÓN DE CERTIFICADOS

• EXPORTAR

Finalmente, para obtener el pfx deberá exportar su certificado:

Ir a Firma electrónica > Certificado electrónico > Exportar

1. Seleccionar el certificado de origen, (*Token e-Sign ANF*)

Certificado electrónico - Exportar

Seleccione forma de exportación

Certificado de origen Formato a exportar

Token e-Sign ANF AC

Ordenador personal

Anterior Aceptar

1. GESTIÓN DE CERTIFICADOS

• EXPORTAR

2. Seleccionar el formato a exportar (PFX)

Certificado electrónico - Exportar

Seleccione forma de exportación

Certificado de origen: Token e-Sign ANF AC Formato a exportar: **Seleccionar**

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB
Windows	Windows		

Relación de certificados almacenados en el dispositivo seleccionado

Datos certificado

Tabla sin contenido

Anterior Aceptar

1. GESTIÓN DE CERTIFICADOS

• EXPORTAR

3. Seleccionar el certificado que desea exportar
4. Presionar aceptar

Certificado electrónico - Exportar

Seleccione forma de exportación

Certificado de origen: Formato a exportar:

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	
Windows	Windows			

Relación de certificados almacenados en el dispositivo seleccionado

Datos certificado
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (CIFRADO)
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (FIRMA)
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (AUTENTICACION)

1. GESTIÓN DE CERTIFICADOS

• EXPORTAR

5. Seleccionar donde desea guardar el certificado
(Es recomendable guardarlo en el mismo Dispositivo eSign).

Certificado Electrónico - Exportar

Seleccione Forma de editar Certificado de Origen Token e-Sign ANF Formato a exportar Seleccione PFX

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño
Plug and Sign	I:\	PLUG&SIGN (I:)	4.0 GB
WINDOWS	WINDOWS		

Relación de certificados almacenados en el dispositivo seleccionado

Datos Certificado

CERTIFICADO DE PERSONA FISICA - NOMBRE APELLIDO APELLIDO (AUTENTICACIÓN)

CERTIFICADO DE PERSONA FISICA - NOMBRE APELLIDO APELLIDO (FIRMA)

CERTIFICADO DE PERSONA FISICA - NOMBRE APELLIDO APELLIDO (CIFRADO)

Guardar en el dispositivo eSign (token)

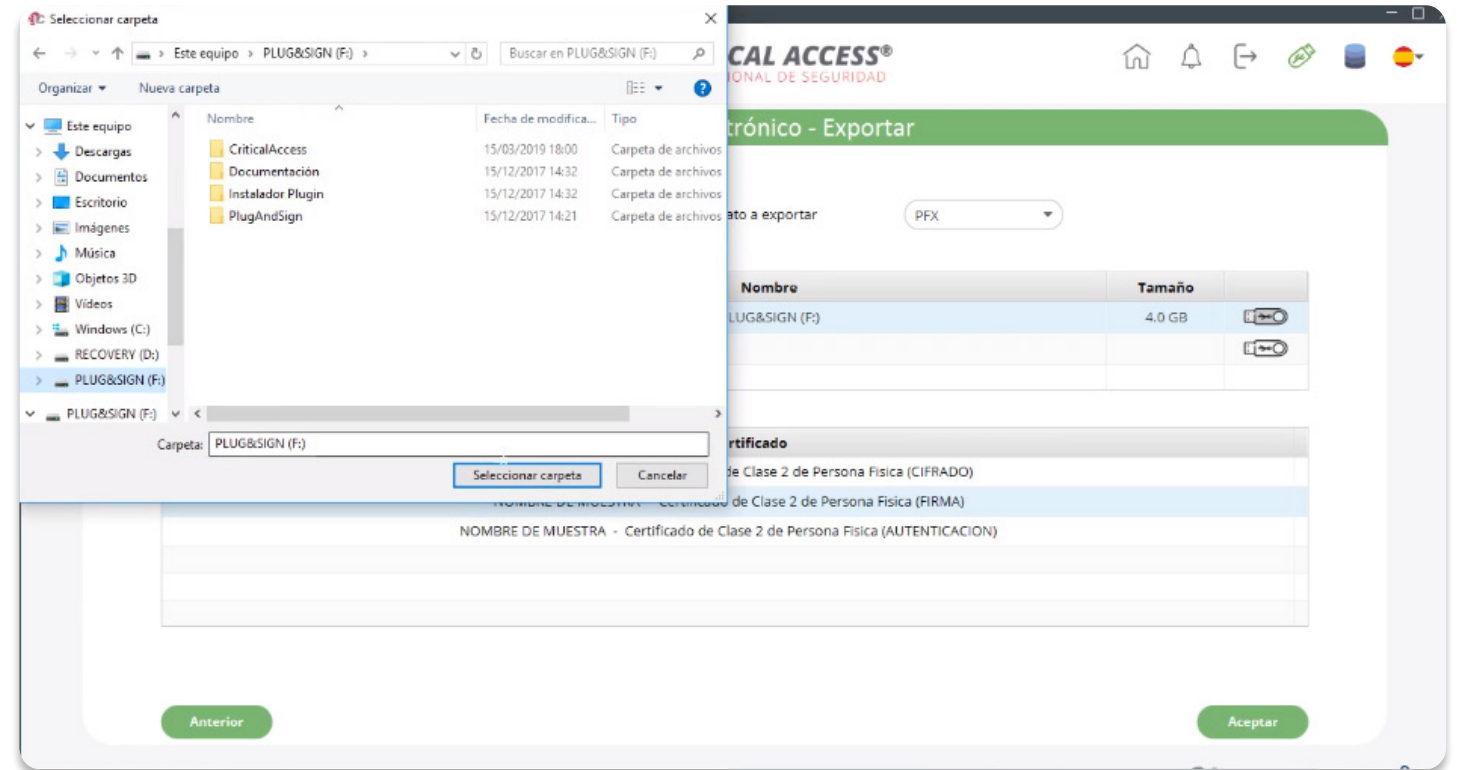
Anterior Aceptar

1. GESTIÓN DE CERTIFICADOS

• EXPORTAR

6. Presionar “Seleccionar carpeta”

Una vez exportado, encontrará el archivo PFX en el lugar donde lo haya exportado. Este es su certificado, deberá instalarlo en el navegador. Puede comprobar los pasos para instalar su certificado en la web de ANF AC www.anf.es



1. GESTIÓN DE CERTIFICADOS

1.2. CAMBIAR PIN

1. Ir a Firma electrónica > Certificado electrónico > Cambio de pin
2. Seleccionar el token y el certificado.
3. Presionar cambio de pin
4. Escribir el PIN antiguo y el nuevo PIN.

Certificado electrónico - Cambio de PIN

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	
Windows	Windows			

Relación de certificados almacenados en el dispositivo seleccionado

Datos certificado

Tabla sin contenido

Anterior

Cambio de PIN

1. GESTIÓN DE CERTIFICADOS

1.3. VER EL LOCALIZADOR Y OTROS DATOS DEL CERTIFICADO

1. Ir a Firma electrónica > Certificado electrónico > Consultar
2. Seleccionar el token correspondiente (donde se encuentra el certificado) y el certificado.

Certificado electrónico - Consultar

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	
Windows	Windows			

Relación de certificados almacenados en el dispositivo seleccionado

Datos certificado
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (CIFRADO)
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (FIRMA)
NOMBRE DE MUESTRA - Certificado de Clase 2 de Persona Fisica (AUTENTICACION)

Anterior

Ver validez

Ver detalles

1. GESTIÓN DE CERTIFICADOS

1.3. VER EL LOCALIZADOR Y OTROS DATOS DEL CERTIFICADO

3. Presionar el botón "Ver detalles"

Certificado electrónico - Consultar

Titular del certificado electrónico		Período de validez del certificado electrónico	
NIF	TINE50000000A	Inicio	Wed Mar 20 14:11:02 CET 2019
Código país	ES	Fin	Fri Mar 19 14:11:02 CET 2021
Nombre común	NOMBRE DE MUESTRA		
Detalles del certificado		DPC y política de certificación	
Entidad emisora	ANF Assured ID CA1	OID Política de certificación	1.3.6.1.4.1.18332.3.4.1.2.22
Número de serie	996984487937917387	Localización de la DCP	http://www.anf.es/documentos
Localizador	133012572-130075795	Aviso al usuario	Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.
Tipo de certificado	Certificado de Clase 2 de Persona Física (FIRMA)	OID Política de certificación	0.4.0.194112.1.0
Usos básicos	Digital signature, Non repudiation		
Usos extendidos	Autenticación web del cliente, Protección de correo electrónico		
Calificación	Reconocido		
Límite de responsabilidad	9 EUR		
Conservación de los datos	15 años		
URL a la PDS	[[https://anf.es/en/, en]]		

Anterior

Actualizar certificado

Exportar a XML

1. GESTIÓN DE CERTIFICADOS


1.4. RENOVAR EL CERTIFICADO

Su certificado tiene una vigencia de 2 años. 30 días antes de la fecha de caducidad recibirá un correo electrónico avisándole de la caducidad próxima y con opción de renovar su certificado por 2 años más, sin necesidad de realizar trámite de identificación... Sin embargo, también puede realizar la renovación directamente desde Suite Critical Access, a partir de 30 días antes de la caducidad:

1. Ir a Firma electrónica > Certificado electrónico > Renovar
2. Seleccionar el token donde se encuentra el certificado a renovar
3. Seleccione el certificado que desea renovar y presionar el botón "renovar"
4. Listo, su certificado ya se encuentra renovado y en un lapso de 24 a 40 horas podrá **descargarlo**. Puede consultar como descargar y exportar su certificado en el apartado "Descargar" y "Exportar".

Certificado electrónico - Renovar

Dispositivos conectados

Modelo	Unidad	Nombre	Tamaño	
Plug and sign	F:\	PLUG&SIGN (F:)	4.0 GB	

Seleccione el certificado que desea renovar

Nombre-OU	Estado
Tabla sin contenido	

Anterior Renovar

1. GESTIÓN DE CERTIFICADOS

1.5. REVOCAR

Puede solicitar la revocación de su certificado desde el apartado "Revocar".

Certificado Electrónico - Revocar

Número de serie del Certificado

[Buscar en la web](#)

Seleccione el dispositivo donde tiene el certificado de firma

Modelo	Unidad	Nombre	Tamaño	
Plug and Sign	I:\	PLUG&SIGN (I:)	4.0 GB	
WINDOWS	WINDOWS			

Seleccione un certificado para realizar la firma

Datos Certificado	

[Anterior](#)
[Siguiente](#)

2. FIRMA ELECTRÓNICA

Desde Suite Critical Access podemos firmar electrónicamente cualquier tipo de archivo. Las firmas aplicadas con este software son consideradas firmas/sellos electrónicos avanzados/cualificados por el Reglamento (EU) No 910/2014, y en cumplimiento con las normas ETSI.

Pulse sobre Firma electrónica > Firmar documentos.

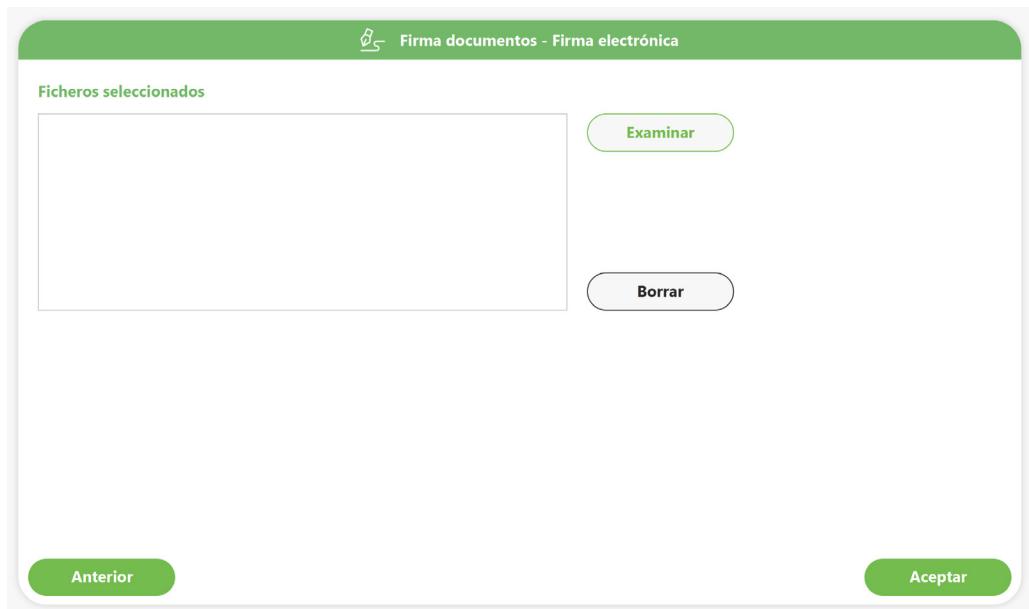
Deberá escoger entre las tres opciones de firma (*Ficheros PDF, Ficheros XML o cualquier fichero*), según el tipo de archivo que vaya a firmar.



2. FIRMA ELECTRÓNICA

2.1. FIRMAR ELECTRONICAMENTE UN DOCUMENTO PDF (PADES)

1. Seleccione el archivo/s (documento PDF) que desea firmar y pulse "Aceptar". Si desea eliminar alguno de los documentos seleccionados, pulse sobre él y seguidamente sobre "Borrar".



2. Seleccione el certificado con el que desea firmar desde la tabla de Certificados Disponibles y muévelo a la tabla Certificados Seleccionados. Seguidamente, pulse "Aceptar".



2. FIRMA ELECTRÓNICA

2.1. FIRMAR ELECTRONICAMENTE UN DOCUMENTO PDF (PADES)

3. Seleccione el tipo de firma que desea aplicar:

- a. Firma básica para PDF (*PAdES B-B*)
- b. Firma para PDF con sello de tiempo (*PAdES B-T*)
- c. Firma para PDF de larga vigencia (*PAdES B-LT*)

4. Pulse sobre "Firmar" y escoja dónde desea guardar el documento firmado.

Una vez acabado el proceso de firma, podrá encontrar el documento PDF firmado en la ruta especificada. A su documento se le habrá aplicado una firma electrónica PAdES en cumplimiento con la normativa europea ETSI EN 319 142.

Firma documentos - Firma electrónica

Firma básica para PDF (*PAdES B-B*)

Firma para PDF con sello de tiempo (*PAdES B-T*)

Firma para PDF de larga vigencia (*PAdES B-LT*)

Anterior Firmar

2. FIRMA ELECTRÓNICA

2.2. FIRMAR ELECTRÓNICAMENTE UN ARCHIVO XML (XADES)

Para firmar un fichero .xml deberá seguir los pasos 1 y 2 del punto anterior 4.1. y, seguidamente:

3. Seleccione el tipo de firma que desea aplicar:
 - a. Firma básica para XML (*XAdES B-B*)
 - b. Firma para XML con sello de tiempo (*XAdES B-T*)
 - c. Firma para XML de larga vigencia (*XAdES B-LT*)

4. Pulse sobre “Firmar” y escoja dónde desea guardar el documento firmado.

Una vez acabado el proceso de firma, podrá encontrar el archivo XML firmado en la ruta especificada. A su documento se le habrá aplicado una firma electrónica XAdES en cumplimiento con la normativa europea ETSI EN 319 132.

2.3. FIRMAR ELECTRÓNICAMENTE CUALQUIER OTRO ARCHIVO (CADES)

Para firmar cualquier otro formato de fichero deberá seguir los pasos 1 y 2 del punto anterior 4.1. y, seguidamente:

3. Seleccione el tipo de firma que desea aplicar:
 - a. Firma básica (*CAdES B-B*)
 - b. Firma con sello de tiempo (*CAdES B-T*)
 - c. Firma de larga vigencia (*CAdES B-LT*)

4. Pulse sobre “Firmar” y escoja dónde desea guardar el documento firmado.

Una vez acabado el proceso de firma, podrá encontrar el archivo firmado en la ruta especificada. A su documento se le habrá aplicado una firma electrónica en cumplimiento con la normativa europea ETSI EN 319 122.

3. VALIDACIÓN DE FIRMAS ELECTRÓNICAS, CERTIFICADOS Y SELLOS DE TIEMPO

Para validar firmas electrónicas pulse sobre:
Firma electrónica > "Verificar".

Encontrará las siguientes opciones para validación:

- **Validación Cualificada:** Validación de la firma de un archivo y obtención de un informe de validación firmado por ANF Autoridad de Certificación, para que el usuario pueda presentarlo directamente como prueba en juicio. Esta opción tiene un coste adicional.
- **Validación Avanzada:** Validación de la firma de un archivo y obtención del resultado en un informe de validación. A diferencia de prueba pericial, este informe no estará firmado por ANF Autoridad de Certificación.
- **Certificado:** Verificación de la cadena de certificados. Se verifica que los certificados de la cadena no estén caducados y que uno sedda emitido por otro dentro de la cadena. Además, se realiza una consulta OCSP para comprobar la vigencia.
- **Sello de tiempo:** Permite verificar un documento sellado con sello de tiempo contra el archivo de sello de tiempo.



3. VALIDACIÓN DE FIRMAS ELECTRÓNICAS, CERTIFICADOS Y SELLOS DE TIEMPO

3.1. VALIDACIÓN CUALIFICADA

1. Pulse sobre “Examinar” para seleccionar el archivo firmado sobre el que quiere realizar la validación de firma. Si desea eliminar alguno de los documentos seleccionados, pulse sobre él y seguidamente sobre “Borrar”.

- Seleccione la opción “Adjuntar certificado de firma” si desea adjuntar los certificados de firma al Informe de validación.
- Seleccione la opción “Documento de validación en formato XML” si desea obtener el informe de validación en formato XML en lugar de PDF (por defecto).

2. Pulse sobre “Verificación de las firmas”.

3. Realice el pago de la validación

4. Obtendrá un informe de validación cualificada de firma electrónica firmado por ANF Autoridad de Certificación en el formato indicado (PDF o XML). Puede extraer ese informe pulsando sobre “Guardar”. También puede extraer el documento original sin la firma pulsando sobre “Extraer documento original”.

✓ Verificación de firmas electrónicas - Validación cualificada

Indique los archivos sobre los que desea realizar la verificación

Examinar

- Haga doble click para visualizar fichero.
- Marque el fichero y pulse borrar si desea modificar selección.

Borrar

Documento de validacion en formato XML

Adjuntar certificados de firma

Anterior

Verificación de Firmas

3. VALIDACIÓN DE FIRMAS ELECTRÓNICAS, CERTIFICADOS Y SELLOS DE TIEMPO

3.2. VALIDACIÓN AVANZADA

Siga los mismos pasos 1 y 2 del punto 4.1.

Seguidamente, obtendrá un informe de validación avanzada de firma electrónica en el formato indicado (*PDF* o *XML*).

Puede extraer ese informe pulsando sobre “*Guardar*”.

También puede extraer el documento original sin la firma pulsando sobre “*Extraer documento original*”.

✓ Verificar eFirmas - Validación Avanzada

Indique los archivos sobre los que desea realizar la verificación

Examinar

- Haga doble click para visualizar fichero.
- Marque el fichero y pulse borrar si desea modificar selección.

Borrar

Documento de validacion en formato XML

Adjuntar certificados de firma

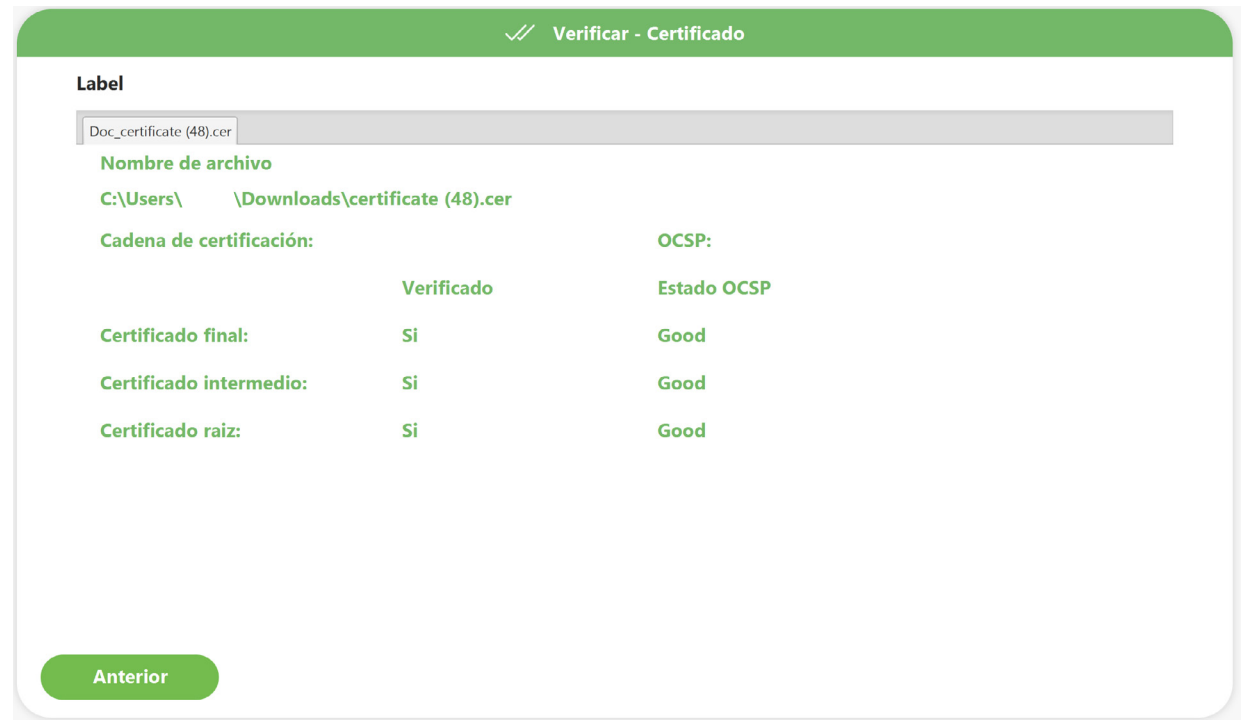
Anterior

Verificación de Firmas

3. VALIDACIÓN DE FIRMAS ELECTRÓNICAS, CERTIFICADOS Y SELLOS DE TIEMPO

3.3. CERTIFICADO

1. Pulse sobre “Examinar” para seleccionar el certificado o certificados sobre el que quiere hacer la verificación de cadena y OCSP. El/los certificado/s deberá tener extensión .cer, .pem, .p7b, .p7c o .pfx.
2. Pulse sobre “Verificar”.
Obtendrá el resultado de la verificación de la cadena de certificación y del estado OCSP. Si ha consultado varios certificados a la vez, estos aparecerán como pestañas en la parte superior.



3. VALIDACIÓN DE FIRMAS ELECTRÓNICAS, CERTIFICADOS Y SELLOS DE TIEMPO

3.4. SELLO DE TIEMPO

1. Seleccione el fichero original que contiene el sello de tiempo.
2. Seleccione el archivo de sello de tiempo .pb7
3. Pulse sobre "Verificar"

Si la verificación es correcta obtendrá el siguiente mensaje:

- La verificación de sello de tiempo fue exitosa.

En caso contrario:

- Verificación Fallida.

The screenshot shows a web interface titled "Verificar - Sello de tiempo". It contains two identical sections for file selection. Each section has a heading "Seleccione el fichero original" followed by a "Fichero seleccionado" label and a dashed rectangular input field. To the right of the input field are two buttons: "Examinar" (green) and "Borrar" (grey). Below each section is another heading "Seleccione el fichero de sello de tiempo" followed by another "Fichero seleccionado" label and a dashed rectangular input field. To the right of this second input field are two buttons: "Examinar" (green) and "Borrar" (grey). At the bottom left of the interface is a green button labeled "Anterior", and at the bottom right is a green button labeled "Verificar".

4. ACTUALIZACIÓN DEL CRITICAL

Nuestros clientes podrán obtener la versión más reciente del Critical Access a través de nuestra página web <https://anf.es/es/> inicio en el apartado de "Catálogo".

Siempre que se vaya a utilizar esta aplicación es necesario verificar en este apartado que se dispone de la última versión del Critical Access.

