Guía práctica para el nuevo perfil de archivero/a ante el archivo digital

Kit de supervivencia

para afrontar los retos de la Ley Foral 9/2026 de Archivos de Navarra



Gobierno de Navarra
Nafarroako Gobernua

Índice

BLOQUE 2. IDENTIDAD ELECTRÓNICA, CERTIFICADOS DIGITALES Y FIRMAS ELECTRÓNICAS **3**

FINALIDAD DEL BLOQUE 4

CONTEXTO Y CONCEPTOS CLAVE 5

1. Identidad digital 6

2. Certificados digitales 8

2.1. Tipos de certificados 8

2.2. Ciclo de vida de los certificados digitales 10

2.3. Actores involucrados en la emisión y uso de los certificados digitales 11

3. Firma electrónica 12

3.1. Formatos de firma 13

3.2. Ampliación de las firmas 13

4. Sello de tiempo 15

PARA SABER MÁS 16

ESCENARIOS Y SITUACIONES HABITUALES 17

Escenario 1. Validación de firmas electrónicas 18

Escenario 2. Preservación de las firmas electrónicas 20

Escenario 3. Documento sin firma electrónica 22

Escenario 4: Identificación y validación de sellos de tiempo 23

Bloque 2

Identidad electrónica, certificados digitales y firmas electrónicas

Finalidad del bloque

Este bloque proporciona el conocimiento esencial sobre identidad electrónica, certificados digitales y firmas electrónicas.



Comprender

conceptos clave de identidad digital, certificados y firmas electrónicas.



Identificar

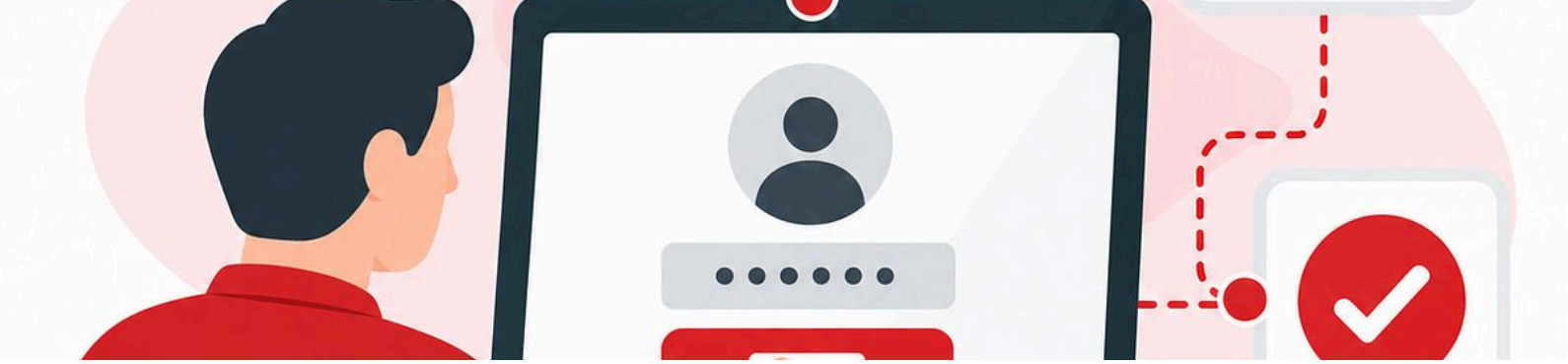
formatos y métodos de validación de firma.



Aplicar

criterios de preservación en el archivo electrónico.

Contexto y conceptos clave



1. Identidad digital

Existen tres tipos de **mecanismos de autenticación** para verificar la identidad en los entornos electrónicos:

Usuario o contraseña, o claves concertadas («Una cosa que yo sé»)

· Se trata del mecanismo más sencillo de todos. A la persona usuaria se le da un nombre público y un código que solo ella conoce y, con la combinación de los dos, se puede identificar. Si nadie más conoce su contraseña, nadie la podrá suplantar.

Inconveniente: todo aquello que pueda ser recordable, como una contraseña, es difícil de sustraer porque se puede memorizar, pero una persona puede perder el control de sus contraseñas fácilmente.

Tokens y sistemas complejos de claves («Una cosa que yo tengo»)

· Son mecanismos como las tarjetas de coordenadas de las entidades bancarias (tokens) o los teléfonos móviles donde, en el momento de identificarnos, se puede enviar una segunda contraseña mediante SMS o se puede disponer de una aplicación que genera esta segunda contraseña.

Inconveniente: estos mecanismos, como los tokens, son fáciles de sustraer. Por eso, la mayor parte de los sistemas de acceso combinan dos factores de autenticación.

Herramientas biométricas («Una cosa que yo soy»)

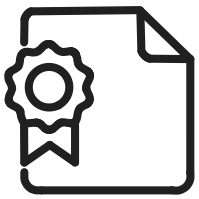
Herramientas como patrones de retina o huella dactilar que se pueden grabar una vez y utilizarse cada vez que se produce la autenticación para comprobar que la persona que se identifica es quien dice ser.

Inconveniente: los datos biométricos se deben almacenar para poder hacer la comprobación y podrían ser exportables para hacer un mal uso. Además, son datos especialmente protegidos por la normativa de protección de datos.

En la relación electrónica administrativa, la Ley 39/2015 (arts. 9 y 10) señala que la identificación de las personas interesadas ante las administraciones públicas puede realizarse mediante certificados digitales, con sistemas de clave concertada o con cualquier otro que las administraciones públicas consideren válido.

En cualquier caso, se trata de sistemas donde existe una relación previa con la persona que se identifica y se ha podido comprobar su identidad antes de facilitarle el medio de identificación.

Se puede identificar y firmar electrónicamente, por ejemplo, con los siguientes medios de identificación:



Certificado digital

Fichero emitido de manera electrónica por una autoridad de certificación que comprueba la identidad de la persona titular.



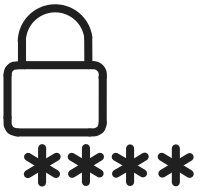
Cl@ve PIN

Sistema basado en un registro previo, por el cual se comprueba la identidad de la persona usuaria y se vincula con un teléfono móvil al cual, mediante la App Cl@ve PIN, se envía una contraseña de validez muy limitada en el tiempo cada vez que requiere utilizar la identidad digital.



Cl@ve Permanente

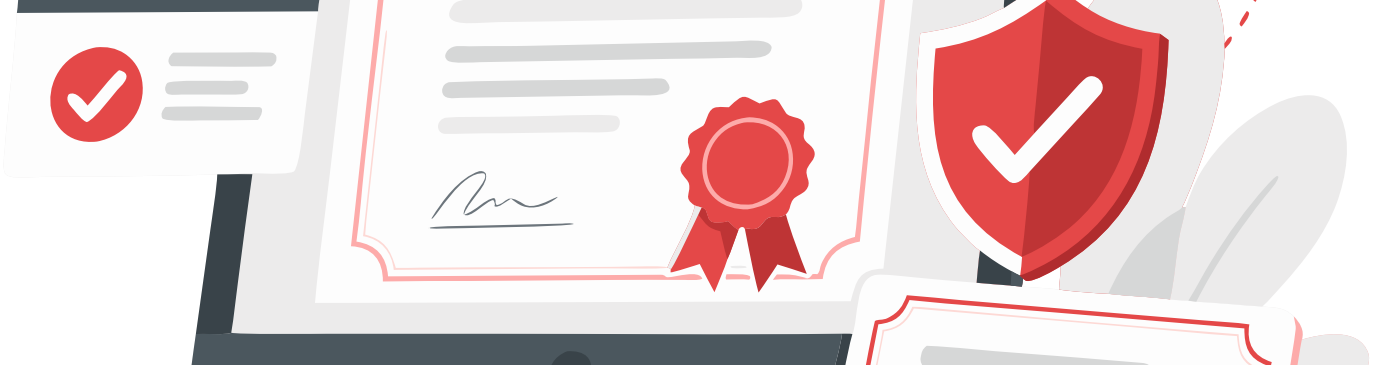
Sistema de contraseña de larga duración basado en un registro previo, por medio del cual se comprueba la identidad de la persona usuaria y se le entrega una contraseña que puede utilizar como identidad digital sin necesitar otro sistema adicional.



Usuario y contraseña

Sistema basado en usuario y contraseña entregada por la propia administración pública mediante un registro previo.

A diferencia del medio de identificación anterior, que es un sistema de la Administración General del Estado, el usuario y contraseña es un sistema de identificación propio de cada administración que tiene que ser autorizado por su Política de firma electrónica y por el Ministerio correspondiente para que se pueda reconocer como un medio válido de identificación.



2. Certificados digitales

El certificado digital o electrónico es un fichero emitido y firmado electrónicamente por una autoridad de certificación que actúa como un tercero de confianza que permite garantizar la identidad de una persona a Internet y, además, vincular unos datos a la persona identificada.

2.1. Tipos de certificados

En función de los atributos y usos, los certificados pueden ser:

Certificado personal

Identificado una persona física y garantiza su identidad, como por ejemplo el DNI-e. En este tipo de certificado aparecerán los datos de la persona titular del certificado digital, nombre completo y número de identificación fiscal.

Certificado de pertenencia a una empresa

Identifica a la persona física que trabaja en una empresa privada. En este tipo de certificado, además de los datos de la persona titular, aparecerán los datos de la entidad a la que pertenecen sin que tenga poderes de representación de la misma.

Certificado de trabajador/a público/a o cargo público

Vincula a una persona con la entidad pública para la cual trabaja. Este tipo de certificado es el mismo que el anterior, pero el cargo y la organización a la que pertenece la persona titular hacen referencia a una entidad pública.

Certificado de representante de persona jurídica

Otorga poder de representación de una persona hacia una entidad pública o privada. En este tipo de certificado, además de los datos de la persona titular, aparecerán los datos de la entidad a la que representan.



Certificado de sello electrónico

Se utiliza en procesos de firma automatizada y se puede asimilar al sello que se usa en el apoyo papel. Solo sirve para acreditar que un proceso automático ha generado un documento, es decir, actuaciones administrativas automatizadas (por ejemplo, firmar el recibo al registro de entrada).



Certificado de servidor seguro

Identifica servidores o aplicaciones informáticas. En el caso concreto de una web o una sede electrónica, permite establecer comunicaciones seguras puesto que garantiza en los suyos la titularidad de la web, es decir, a quien pertenece, y protege la integridad de la información intercambiada.

En función del **soporte**, los certificados pueden ser:



Certificados en software

La mayoría de los certificados que se emplean son de este tipo. Sus características son:

- No requieren el uso de hardware adicional.
- Pueden ser utilizados en diferentes dispositivos, incluidos los móviles.
- Solo permiten la generación de firmas avanzadas por el hecho de que teniendo acceso al certificado digital, cualquier persona lo podría utilizar sin otro factor de identificación.



Certificados almacenados en un chip criptográfico

Un ejemplo sería el DNI electrónico. Sus características son:

- Requieren de un dispositivo capaz de operar con el chip criptográfico.
- La clave privada no se puede extraer del chip.
- Para su uso se requiere de la autenticación mediante un PIN.
- Permiten la generación de firmas cualificadas por el hecho que solo se pueden generar si se dispone de acceso al chip criptográfico y se conoce el PIN.



Tecnología HSM, o Hardware Security Model (en la nube)

Se trata de un repositorio seguro de certificados en la nube al que se puede acceder de forma remota desde diferentes dispositivos, de modo que la persona titular del certificado no ha de disponer de un objeto físico en el que almacenar su certificado para usarlo para firmar. Sus características son:

- Gestiona certificados que no pueden ser exportados y, por lo tanto, permite generar firmas cualificadas.
- Permite compartir el uso del certificado digital, guardando un registro de todos los usos y pudiendo limitar las webs en las que se puede emplear.

2.2. Ciclo de vida de los certificados digitales

Las etapas del ciclo de vida de los certificados digitales son las siguientes:

Emisión

Proceso por el cual se emite el certificado digital una vez verificada la identidad de su titular y los datos vinculados como por ejemplo el nivel de representación o de vinculación con una entidad.

Renovación

Emisión de un certificado con los mismos datos, renovando únicamente las claves para alargar su vida útil. Se puede realizar de manera remota, a pesar de que está limitada a un número determinado de iteraciones después de las cuales habrá que repetir el proceso de acreditación ante la Autoridad de Certificación de la identidad y de la información que contiene el certificado digital.

Caducidad

El certificado caduca automáticamente pasado un tiempo. Esta información se encuentra en el mismo certificado.

Suspensión

Revocación con carácter temporal y reversible porque el certificado no será necesario durante un determinado periodo de tiempo, por ejemplo, en el caso de baja laboral de larga duración. Es una medida preventiva para evitar un mal uso en periodos largos de tiempos que se prevé que el certificado no será necesario.

Revocación

Negación de la validez del certificado por parte de su titular, ya sea porque su seguridad se ha visto comprometida o porque la información que contiene ya no es correcta.

2.3. Actores involucrados en la emisión y uso de los certificados digitales

Durante el ciclo de vida de los certificados digitales intervienen una serie de **actores**:

Autoridad de certificación

Organización responsable de la seguridad criptográfica del sistema.

Garantiza la cadena de confianza y emite los certificados digitales.

Entidad de registro

Oficina a la que se dirige el particular para obtener un certificado.

Llega previamente a un acuerdo con la Autoridad de certificación para validar la identidad de los titulares y ofrecer los certificados sin necesidad que la persona interesada deba dirigirse directamente a la Autoridad de certificación.

Mientras que la Autoridad se encarga de la seguridad tecnológica, la Entidad de registro se encarga de la identificación de las personas interesadas.

Validador

Entidad que recibe el documento firmado.

Su confianza en la firma depende de que confíe en la Autoridad de certificación.



3. Firma electrónica

La firma electrónica es un conjunto de información que se adjunta a un documento electrónico y que permite garantizar la integridad y la autenticidad del documento.

Esta información se genera a partir del contenido del documento y de la clave privada del certificado digital con el cual se realiza la firma electrónica, de modo que cualquier modificación del documento, aunque sea únicamente añadir un espacio en blanco, puede ser detectada e invalidar la firma.

Firma electrónica simple

- Datos electrónicos que emplea una persona para firmar.
- Con efectos jurídicos.
- Puede ser admitida como prueba en un procedimiento judicial, aunque se necesitarían pruebas complementarias.

Firma electrónica avanzada

- Vinculada al firmante de forma única.
- Permite la identificación del firmante.
- El firmante tiene bajo su control los datos de creación de la firma.
- Modificaciones posteriores a la firma son detectables.

Firma electrónica cualificada

- Creada mediante un dispositivo de creación de firmas electrónicas cualificado.
- Basada en un certificado electrónico cualificado de firma electrónica.
- Tiene el mismo efecto jurídico que la firma manuscrita.

3.1. Formatos de firma

Dependiendo del formato, las firmas electrónicas pueden ser:

Firma adjunta (*attached*)

La firma se encuentra incrustada dentro del mismo documento, de modo que este incluye la información sobre la firma y el certificado digital.

Es la firma más habitual, utilizada con frecuencia en documentos de oficina (PDF, Word, Open Office).

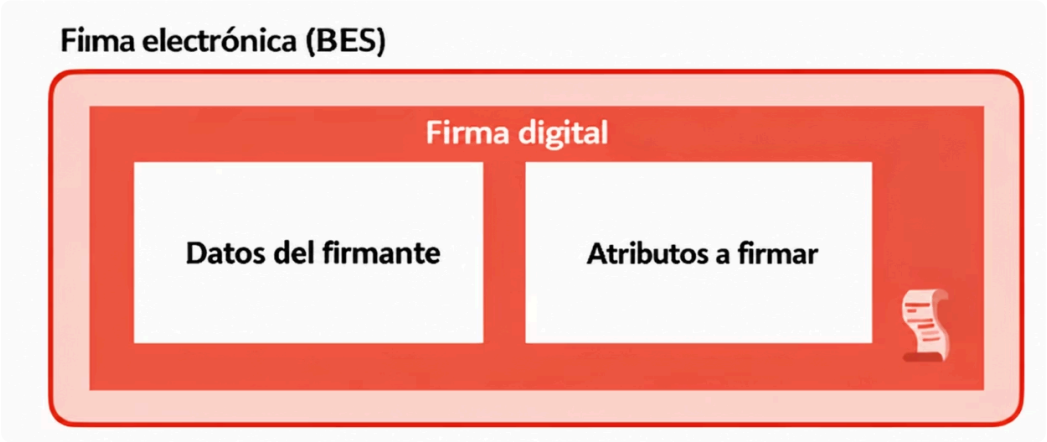
Firma separada (*detached*)

La firma y la información del certificado se guardan en un objeto digital separado. Permite firmar cualquier tipo de objeto digital. Muy útil para formatos que no admiten firmas adjuntas (fotografías, vídeos, planos…).

En estos casos se dispone de dos archivos: el documento firmado y el documento con la firma.

3.2. Ampliación de las firmas

Cualquier firma electrónica tendrá los datos del firmante, la información que firma (el resumen criptográfico) y un criptograma. Se trata de los elementos de la **firma electrónica más básica (Basic Electronic Signature – BES).**

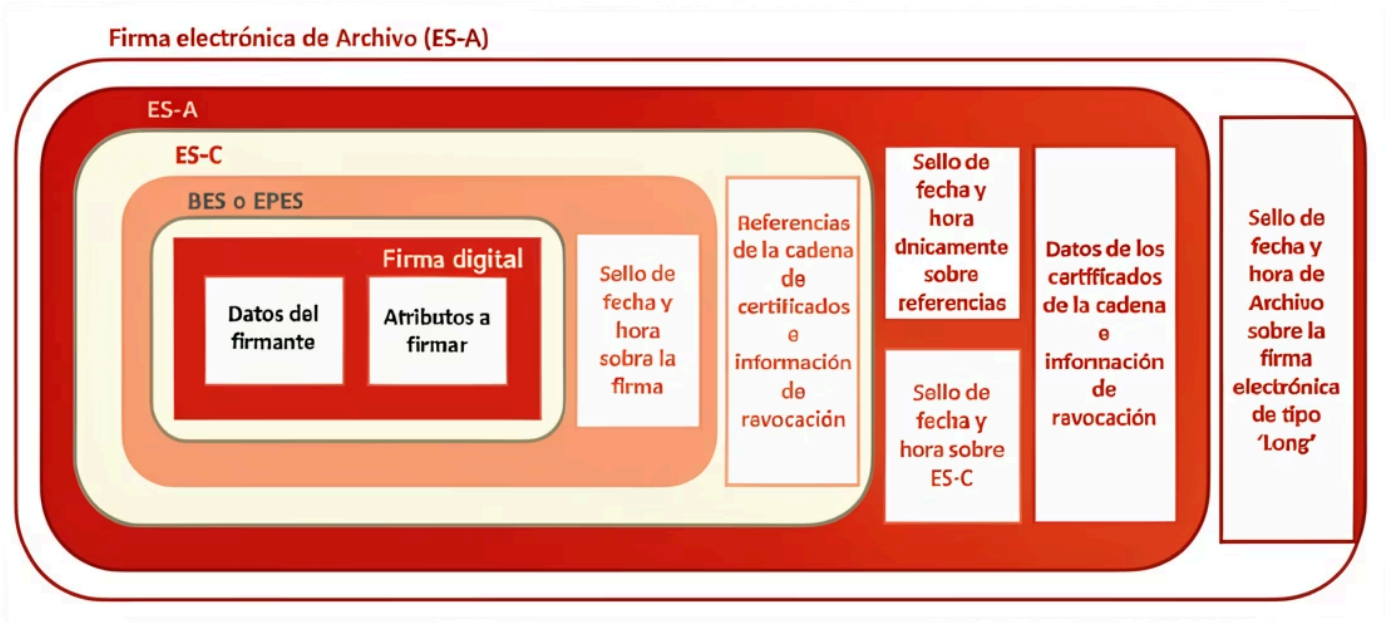


Esta estructura se puede ampliar para generar más información. La firma *attached* es más flexible en cuanto a su gestión y completación. El estándar XAdES, por ejemplo, ofrece diferentes mecanismos para añadir a una firma *attached* información sobre la validación de la vigencia o el sellado de tiempo para confirmar la fecha en que se ha realizado la comprobación.

Las extensiones se pueden describir en formato **PDF** (**PAdES**), **XML** (**XAdES**) o **CMS** (**CAdES**). De este modo, por ejemplo, a una firma básica se le puede añadir un sello de fecha y hora, obteniendo como resultado una firma de tipo -T (**PAdES-T, XAdES-T** o **CAdES-T**). Si a esta se le añaden, además, referencias de la cadena de certificados e información de revocación, así como un sellado de tiempo, se obtendrá una firma **-XL**.

Si se conserva toda la información necesaria para efectuar todas las verificaciones del certificado, e incluso de la existencia de la Autoridad de certificación cuando esta haya dejado de existir, se convertirá en una **firma de archivo (-A)**. Este tipo de firma prevé la posibilidad de que cualquier Autoridad de certificación pueda dejar de existir en un futuro, de modo que el documento deberá contener toda la información relativa a la Autoridad (por qué podía emitir certificados, por ejemplo) y a los certificados (si eran válidos, si habían sido revocados...).

Para **cada tipo de actuación se escoge un tipo de firma**. Por ejemplo, para aquellas actuaciones que no van a prolongarse mucho en el tiempo, se utilizarán firmas básicas; para las que duren años, firmas con sellado de tiempo; y cuando se prolonguen de manera infinita, firmas de tipo -A.





4. Sello de tiempo

Los sellos de tiempo son mecanismos que certifican la existencia de datos electrónicos en un momento específico, garantizando que no han sido modificados desde entonces.

Los sellos de tiempo se incorporan en las firmas electrónicas, de modo que se pueda acreditar:

Que una firma electrónica se realizó en un momento concreto y no antes o más tarde, lo cual permite comprobar, a su vez, que el certificado electrónico con el que se emitió la firma estaba vigente en el momento de la firma.

La fecha en que una información concreta ha sido registrada, publicada, despublicada... a efectos de acreditar el cumplimiento de plazos ante terceros. Por ejemplo, la entrada de un documento en un registro administrativo o una publicación en la sede electrónica.

Para saber más

Normativa

- Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónico.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.

Escenarios y situaciones habituales

Escenario 1. Validación de firmas electrónicas

Situación

El archivo electrónico recibe documentos firmados electrónicamente —ya sea a través de transferencias procedentes del gestor de expedientes de la organización o de ingresos manuales.

Estas firmas pueden haber sido realizadas mediante:

- Certificados digitales.
- Actuación administrativa automatizada (sellos electrónicos de órgano o CSV).
- Identificación más voluntad de firma (Cl@ve).

La herramienta de archivo electrónico realiza las comprobaciones de la validez de las firmas electrónicas de forma automática, pero es posible que se produzca algún error. En este caso, las firmas deben validarse de forma manual.

Decisiones operativas

Si la firma electrónica ha sido realizada mediante CSV:

- Se debe acceder a la página web de la administración emisora del documento y, desde el validador de CSV, incorporar el CSV y descargar el documento que el validador devolverá. Este documento se deberá adjuntar al expediente.

Si la firma electrónica ha sido realizada mediante un sistema de identificación y voluntad de firma:

- El documento estará firmado con un sello electrónico y se deberá proceder como se indica en el siguiente punto.
- Además, se deberá contactar con la persona responsable de la plataforma de administración electrónica de la organización para que indique dónde se almacena la evidencia de la identificación y de la voluntad de firma, ya que se trata del sistema mediante el cual se realiza la firma y, por lo tanto, dicha evidencia deberá guardarse en el expediente.

Si la firma electrónica ha sido realizada mediante un certificado digital o un sello electrónico:

1. Validar la firma electrónica mediante una herramienta externa de validación:

a. Si el certificado ha sido emitido por un **prestador de servicios de confianza de España,** se puede utilizar la plataforma **VALIDe** (AGE): **https://valide.redsara.es/valide/validarFirma/ejecutar.html**

b. Si el certificado ha sido emitido por un **prestador de servicios de confianza de la Unión Europea,** se puede utilizar la plataforma **DSS Demonstration WebApp,** de la Comisión Europea: **https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation**

c. Si el certificado **no ha sido emitido por ningún prestador de servicios de confianza de la Unión Europea**, se deberá contactar con el área encargada de sistemas informáticos de vuestra organización.

2. Comprobar el estado del certificado.

La propia herramienta de validación ofrecerá información sobre la firma electrónica y los motivos por los que esta no es válida:

1. **Si el certificado no ha sido emitido por ningún prestador de confianza,** la firma no podrá considerarse válida. En estos casos, la persona profesional de Archivo deberá tomar una de las siguientes decisiones:
   a. Devolver el documento y no aceptar la transferencia porque existen deficiencias.
   b. Aceptar el documento anotando que, cuando ingresó al archivo electrónico, tenía estas deficiencias.
2. **Si el certificado ha sido emitido por un prestador de confianza y ha caducado en el momento de la validación, pero era válido cuando se realizó la firma**, esta última se considerará válida. En estos casos, se anotará en la herramienta que, cuando se transfirió el documento, la firma electrónica no era válida, pero que la organización tiene constancia por otros medios de que, en el momento de la firma, esta era válida.

Escenario 2. Preservación de las firmas electrónicas

Situación

Los documentos administrativos deben conservarse durante largos periodos de tiempo. A la larga, puede producirse:

- Caducidad de los certificados digitales con los que se realizó la firma electrónica.
- Obsolescencia de algoritmos.
- Obsolescencia de formatos de firma electrónica.

Decisiones operativas

Existen dos mecanismos de preservación de las firmas electrónicas:

1. Utilizar formatos de firma longeva y resellado.

Este mecanismo de preservación es el más habitual y extendido.

Existen formatos longevos para evitar que las firmas electrónicas pierdan su validez a largo plazo. Son los formatos tipo **-LTV (PAdES-LTV)** o **-A (XAdES-A),** que permiten añadir evidencias temporales.

Para ello, y en el caso de que el archivo electrónico no disponga de firmas electrónicas en estos formatos, podéis completar las firmas electrónicas en dichos formatos, de modo que:

- XAdES-A para los documentos en formato XML con firma XAdES.
- PAdES-LTV para los documentos en formato PDF o PDF/A.
- CAdES-A para los documentos en cualquier formato con firma CAdES.

> **Las personas profesionales de archivo se pueden poner en contacto con el proveedor de la herramienta o con el área encargada de sistemas informáticos de la organización si necesitan soporte en esta tarea.**

Una vez completadas las firmas a estos formatos longevos, el archivo electrónico detectará de forma automática el momento en el que los sellos electrónicos estén a punto de caducar para resellar las firmas electrónicas mediante la aplicación de un nuevo sello, con una caducidad suficiente y con los algoritmos o claves de firma actualizados.

⚠ **Hay herramientas de archivo electrónico que únicamente aplican el resellado sobre el índice de los expedientes y no sobre cada uno de los documentos que lo conforman.**

Esta opción sería igualmente válida, pero os deberéis asegurar que el índice del expediente está en formato XAdES-A.

No obstante, hay que tener en cuenta que, cuando un tercero solicite un documento de un expediente:

- Se le remitirá todo el expediente porque la integridad de la firma no se encuentra en el documento, sino en el índice del expediente.
- Se le remitirá el documento solicitado junto con el índice, en el caso de que el expediente no pueda compartirse en su totalidad.

2. Almacenamiento de los documentos y sus firmas en un archivo electrónico único.

La otra forma de garantizar la autenticidad de los documentos, con independencia de si se preservan o no sus firmas electrónicas, es **declarar formalmente que el archivo electrónico es un archivo electrónico único** y que, por lo tanto, es una herramienta segura.

Esta alternativa de preservación está alineada con lo establecido en el artículo 22.4 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, según el cual:

> Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, estas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Escenario 3. Documento sin firma electrónica

Situación

El archivo electrónico recibe documentos sin firma electrónica –ya sea a través de transferencias procedentes del gestor de expedientes de la organización o de ingresos manuales.

Decisiones operativas

1. Verificar la normativa interna.

Las personas profesionales de archivos deben identificar si el documento en cuestión requiere firma electrónica. Para ello, deberán revisar la normativa interna (Reglamento de administración electrónica o similar y/o Política de firma electrónica) y comprobar si los documentos procedentes de fuentes externas o los documentos generados internamente requieren firma electrónica, independientemente de la tipología documental de la que se trate.

2. Devolver el documento al área tramitadora o aceptar el ingreso al archivo electrónico.

En el caso que el documento en cuestión **requiera firma electrónica, y si se trata de un documento generado internamente**, las personas profesionales de archivos no podrán aceptar la transferencia y devolverán el expediente al área tramitadora, con indicación de la necesidad de incorporar una firma electrónica.

En el caso que el documento en cuestión requiera firma electrónica, pero proceda de **fuentes externas**, se identificará como copia simple (EE99 – Otros) mediante el metadato eEMGDE20 – Estado de elaboración.

Escenario 4. Identificación y validación de sellos de tiempo

Situación

El archivo electrónico recibe documentos firmados electrónicamente —ya sea a través de transferencias procedentes del gestor de expedientes de la organización o de ingresos manuales—, y estos pueden incorporar sellos de tiempo.

El sello de tiempo ofrecerá la seguridad fidedigna del momento en el que se produjo la firma electrónica y, si existiesen problemas con la caducidad del certificado de las firmas, el sello de tiempo será un mecanismo que permitirá acreditar que el certificado era vigente en la fecha de emisión de la firma.

En la gran mayoría de los casos, la herramienta de archivo electrónico realizará las comprobaciones de la validez de los sellos de tiempo de forma automática. No obstante, es posible que las personas profesionales de archivos deban efectuar una validación de estos de forma manual, de modo que deberán saber identificarlos y validarlos.

Decisiones operativas

1. Comprobación de la existencia del sello de tiempo.

Para comprobar la existencia de sellos de tiempo, se pueden utilizar:

1. **Adobe Acrobat Reader** (para los documentos en PDF). Al abrir el documento con este visor, se identificará de forma automática si se dispone de sello de tiempo y se podrá obtener información sobre dicho sello.
2. **Herramientas de validación de firmas electrónicas**. Como en el caso de la validación de las firmas electrónicas (escenario 1), para la comprobación e identificación de los sellos de tiempo también se podrá recurrir a este tipo de herramientas:
    - **VALIDe:** https://valide.redsara.es/valide/validarFirma/ejecutar.html
    - **DSS**: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation

2. Identificación del tipo de sello de tiempo: cualificado o no cualificado.

Las herramientas de validación podrán indicar si se trata de un sello de tiempo cualificado o no, lo que ofrecerá mayores o menos garantías de seguridad jurídica del documento:

Sello de tiempo cualificado

Ha de cumplir con una serie de requisitos establecidos en el Reglamento eIDAS:

- Ha sido emitido por un prestador de servicios de confianza cualificado.
- Permite vincular la fecha y hora con los datos firmados, de forma que se garantizará que los datos no han sido modificados desde la incorporación del sello.
- Ofrece una hora basada en una fuente de información temporal vinculada al Tiempo Universal Coordinado, como el Real Observatorio de la Armada, que proporciona la base de la hora legal en todo el territorio nacional.

Sello de tiempo no cualificado

Se caracteriza por lo siguiente:

- Puede ser emitido por cualquier prestador de servicios de confianza (no ha de ser cualificado).
- La fiabilidad de que los datos no han sido modificados desde la incorporación del sello dependerá de la confianza depositada sobre el prestador de servicios que lo ha emitido.

3. Validación del sello de tiempo

En el caso de emplear herramientas externas, estas ya ofrecerán información suficiente para validar el sello de tiempo y comprobar si se trata de un sello cualificado o no cualificado:

- **Prestador.** Se puede consultar si está incluido en la TSL, o Lista de confianza de prestadores cualificados de servicios electrónicos de confianza del Ministerio correspondiente, disponible desde el siguiente enlace: **https://sedediatid.digital.gob.es/Prestadores/Paginas/Inicio.aspx**
- **Vigencia del sello de tiempo.** Se indicará si el sello de tiempo está vigente o si ha caducado.