
# Manual de validación de firmas electrónicas

**Universidad Politécnica de Madrid**
http://www.upm.es
https://sede-electronica.upm.es

**Edición:** 1.1
**Fecha:** 05-03-2012

Con la colaboración de:


El Ministerio de Industria, Turismo y Comercio ha financiado parcialmente las actuaciones que la Universidad Politécnica de Madrid ha realizado para la puesta en marcha de los servicios de Administración Electrónica en esta Plataforma (Convocatoria 1/2009 del Plan AVANZA, subprograma Avanza Servicios Públicos Digitales, proyecto Tramita UNI-MADRID TSI-050200-2009-181).



Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U.
CIF: A-78053147
C/ Sor Ángela de la Cruz nº 3, Madrid 28020
Tlf. 91 337 54 00 Fax 91 337 54 78

# Índice

# 1. Introducción

El objeto del presente documento es servir de guía al usuario para la validación de documentos electrónicos firmados digitalmente expedidos por la Plataforma de Tramitación Electrónica de la Universidad Politécnica de Madrid.

Puede encontrar documentación adicional de ayuda y soporte sobre la Sede Electrónica y la Plataforma de Tramitación Electrónica de la Universidad Politécnica de Madrid en la URL siguiente:

https://sede-electronica.upm.es/Ayuda

# 2. Descripción y obtención de los documentos electrónicos

La Sede Electrónica de la Universidad Politécnica de Madrid, en el caso de que expida un documento firmado electrónicamente (como un resguardo de presentación en el Registro Electrónico, una Hoja de Servicios o una Certificación Académica Personal) puede proporcionar:

- Una copia electrónica del documento, que incluye **un código seguro de verificación** impreso al pie del propio documento, que le confiere el carácter de copia auténtica del original. Esto es así porque dicho código seguro de verificación permite acceder en todo momento al documento original mediante un formulario preparado al efecto en la Sede Electrónica de la Universidad Politécnica de Madrid. En la ***Figura 1*** se muestra el pie de una copia electrónica de un documento presentado en el Registro Electrónico de la UPM, en el que puede observarse el código seguro de verificación (aparece dos veces, rodeado por una línea roja). Este documento es un archivo PDF (ISO 32000).

- El documento electrónico original, sin incluir ni las firmas electrónicas ni los certificados correspondientes. Es también un archivo PDF (ISO 32000).

- Un fichero con las firmas digitales correspondientes asociadas al documento y los certificados de los firmantes. Se trata de firmas electrónicas separadas ("*detached signatures*"), y el archivo sigue el estándar PKCS#7.

Es decir, tras la realización de un trámite, el usuario puede obtener hasta tres archivos correspondientes al mismo documento, que denominaremos en lo sucesivo, respectivamente, `copia.pdf`, `original.pdf` y `firma.p7s`.


*Figura 1 Código seguro de verificación en el pie de una copia electrónica de un documento*

# 3. Procedimientos de validación

La comprobación de la integridad y autenticidad de las copias de ciertos documentos firmados electrónicamente obtenidas durante el proceso de acceso a los servicios electrónicos proporcionados por una Sede Electrónica puede realizarse a través de un *código seguro de verificación* que se proporciona impreso en la copia del propio documento. Esta validación es la más sencilla, pero para ella es necesaria la confianza del usuario en la información proporcionada por la Sede Electrónica, de la que es responsable su titular, la Universidad Politécnica de Madrid.

Adicionalmente, puede realizarse por el usuario una validación minuciosa del documento firmado electrónicamente, que comprende las siguientes acciones:

- Validación de que el documento electrónico se corresponde y no se ha modificado desde que se firmó electrónicamente por el firmante.
- Validación de que el documento electrónico fue firmado por el firmante cuyo certificado está incluido en el fichero de firma.
- Validación del certificado X.509 empleado por el firmante: integridad, periodo de validez y estado de revocación. Tanto el periodo de validez como el estado de revocación del certificado se comprueban frente a la fecha actual en caso que la Firma Electrónica no posea sello de tiempo o frente a dicho sello en caso contrario.

Esta validación puede realizarse mediante el servicio VALIDe, proporcionado por el Ministerio de Política Territorial y Administración Pública o puede realizarla el propio usuario utilizando algunas aplicaciones existentes en el mercado, tanto comerciales como libres. En este documento ilustraremos este proceso con dos de ellas, distribuidas gratuitamente: “openssl” y “XolidoSign” . En el caso de que la validación la realice el usuario, puede que no sea posible realizarse en todos sus pasos, como por ejemplo, validar el estado de revocación del certificado del firmante.

El mecanismo de validación recomendado es el empleo del servicio VALIDe, cuando no sea suficiente el acceso al original mediante el código seguro de verificación en la Sede Electrónica.

## 3.1. Validación mediante la Sede Electrónica de la UPM

En el caso de disponer de una copia electrónica, su validez puede comprobarse mediante el código seguro de verificación incluido en ella, puesto que con él la Sede permite descargar el documento original y el fichero de firmas asociado. En todo caso, la propia presencia del documento en la Sede Electrónica debería ser garantía de su autenticidad, ya que legalmente “*el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma*”. Por tanto es la propia Universidad Politécnica de Madrid la que responde de la veracidad y autenticidad de los documentos descargados de su Sede Electrónica mediante un código seguro de verificación impreso en una copia electrónica.

En el caso de disponer del código seguro de verificación que se muestra en la *Figura **1***, puede accederse a la URL, accesible también desde la Sede Electrónica, siguiente:

https://e-administracion.upm.es/verificadorFirmas

Como se muestra en la *Figura* ***2***, aparecerá un formulario en el que debe incluirse el código seguro de verificación y un conjunto de caracteres de seguridad que se muestran en una imagen distorsionada en pantalla ("*CAPTCHA*").


*Figura 2 Formulario para la verificación de documentos electrónicos*

Tras pulsar en el botón "*Buscar*", se presentará al usuario lo mostrado en la *Figura **3***.


*Figura 3 Pantalla de descarga del documento electrónico original y del fichero de firmas asociado*

Pulsando en el botón "Descargar Documento" podremos acceder y descargar el documento electrónico original (que hemos denominado `original.pdf`). Además, pulsando en el icono con la flecha roja (rodeado en rojo en la figura) podremos descargar el fichero de firmas asociado (que hemos denominado `firma.p7s`).

## 3.2. Validación mediante el servicio VALIDe

El Ministerio de Política Territorial y Administración Pública proporciona de manera general y gratuita el servicio **VALIDe**, que permite comprobar la validez de la firma en cualesquiera documentos electrónicos firmados digitalmente. La validación realizada por este servicio es la más completa posible, ya que realiza todas las acciones enumeradas anteriormente, incluido el estado de revocación del certificado del firmante, comprobándose además que el certificado y su emisor sean reconocidos y soportados por la Plataforma VALIDe.

Para validar un documento, en primer lugar debe accederse al servicio, mediante la URL:

https://valide.redsara.es/valide/pages/irValidarFirma

En el formulario proporcionado, mediante el botón “Examinar” debe proporcionarse el fichero de firma separada PKCS#7 (`firma.p7s`) y el código de seguridad consistente en un conjunto de caracteres que se muestran en una imagen distorsionada en pantalla (“*CAPTCHA*”). Finalmente debe pulsarse el botón “VALIDAR. Estos pasos se muestran en la *Figura **4***.


*Figura 4 Pantalla de acceso al servicio de validación de firmas de VALIDe*

Como resultado de esta acción se mostrará la pantalla que se ilustra en la *Figura **5***. El texto mostrado en color rojo **no es un mensaje de error**, simplemente avisa de que el fichero proporcionado (`firma.p7s`) no contiene al documento (por tratarse de un fichero de firma separada PKCS#7). De manera análoga al paso anterior, debe proporcionarse al sistema el citado documento electrónico (`original.pdf`) y un nuevo código de seguridad (“*CAPTCHA*”). Pulse “VALIDAR” de nuevo.


*Figura 5 Pantalla de selección del documento electrónico original*

Finalmente, se presentará al usuario el resultado de la validación. Pulsando sucesivamente los botones “Detalle de la validación” y “Detalle de los firmantes” se mostrará una pantalla como la de la *Figura* ***6***, en la que figuran los ficheros correspondientes, la fecha y hora de la firma del documento, los firmantes e información relativa a los certificados de los firmantes.

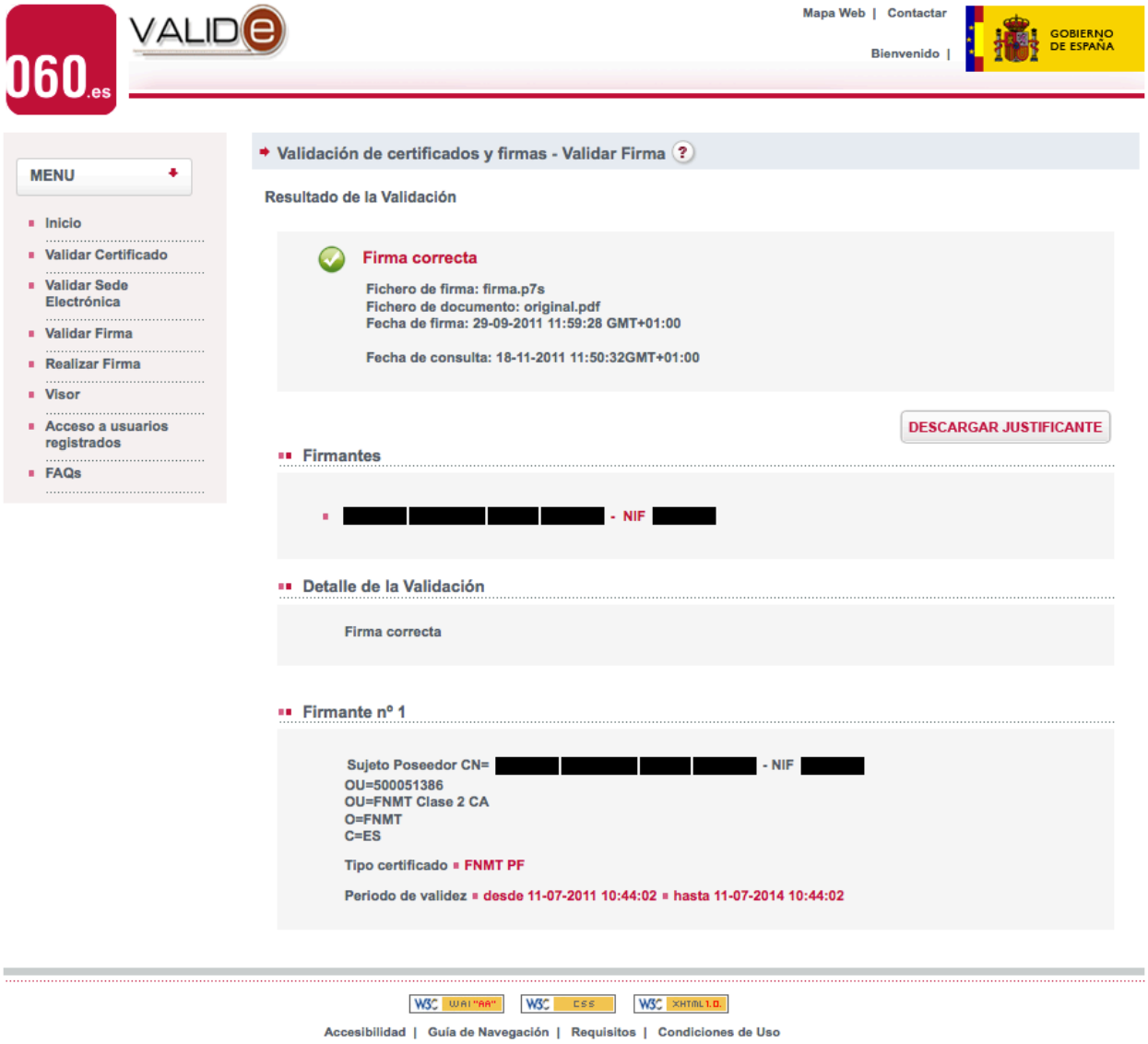


*Figura 6 Resultado de la validación del documento electrónico*

## 3.3. Validación mediante *openssl*

Openssl es un proyecto colaborativo para la implementación de un conjunto de herramientas completo, robusto y de fuentes abiertas, que implementa los protocolos SSL (v2/v3) y TLS (v1), así como una completa librería criptográfica de propósito general. Por tratarse de una herramienta de fuentes abiertas pueden encontrarse distribuciones preparadas para diferentes sistemas operativos.

El proceso de validación de un documento firmado electrónicamente puede realizarse como sigue:

***Validación de los certificados incluidos en el fichero de firma PKCS#7***

El comando siguiente muestra los detalles de los certificados intervinientes en la firma (certificado del firmante y certificado de la autoridad de certificación correspondiente). En el resultado puede verse la identificación del firmante (NOMBRE y NIF borrados en el ejemplo).

```
openssl pkcs7 -in firma.p7s -inform DER -print_certs -text
```

El resultado que se obtiene es (se muestra parcialmente):

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1020371972 (0x3cd1a404)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, O=FNMT, OU=FNMT Clase 2 CA
        Validity
            Not Before: Jul 11 08:44:14 2011 GMT
            Not After : Jul 11 08:44:14 2014 GMT
        Subject: C=ES, O=FNMT, OU=FNMT Clase 2 CA, OU=500051386, CN=NOMBRE - NIF
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b9:47:cc:65:d1:cb:8b:e0:5d:d2:2b:64:f8:d7:
                    ..............
                    ..............
                    ..............
                    ..............
                    ..............
  Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 921770777 (0x36f11b19)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, O=FNMT, OU=FNMT Clase 2 CA
        Validity
            Not Before: Mar 18 14:56:19 1999 GMT
            Not After : Mar 18 15:26:19 2019 GMT
        Subject: C=ES, O=FNMT, OU=FNMT Clase 2 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:98:3f:ad:19:36:93:3d:3e:fe:76:42:14:fd:35:
                    ..............
                    ..............
                    ..............
                    ..............
                    ..............
```

***Validación de la firma contenida en el fichero de firma PKCS#7***

El comando siguiente comprueba que la firma y los certificados que contiene el fichero `firma.p7s` están vinculados a los datos contenidos en el documento electrónico `original.pdf`. El comando no puede comprobar si el certificado del firmante ha sido o no revocado. Tampoco presenta la fecha y hora en que se realizó la firma electrónica.

```
openssl smime -verify -in firma.p7s -inform DER -content original.pdf  > /dev/null
```

Si la validación es correcta se obtiene:

```
Verification successful
```

## 3.4. Validación mediante *XolidoSign*

XolidoSign es una herramienta que se distribuye gratuitamente y que permite realizar operaciones de firma electrónica, sellado de tiempo y verificación de firmas.

La validación del documento electrónico puede realizarse siguiendo los pasos que ilustran las figuras que siguen:

1. Abrir la aplicación y pulsar el botón “Verificar” (bien en el menú de la izquierda o bien arriba a la derecha, ambos marcados en la figura en rojo).

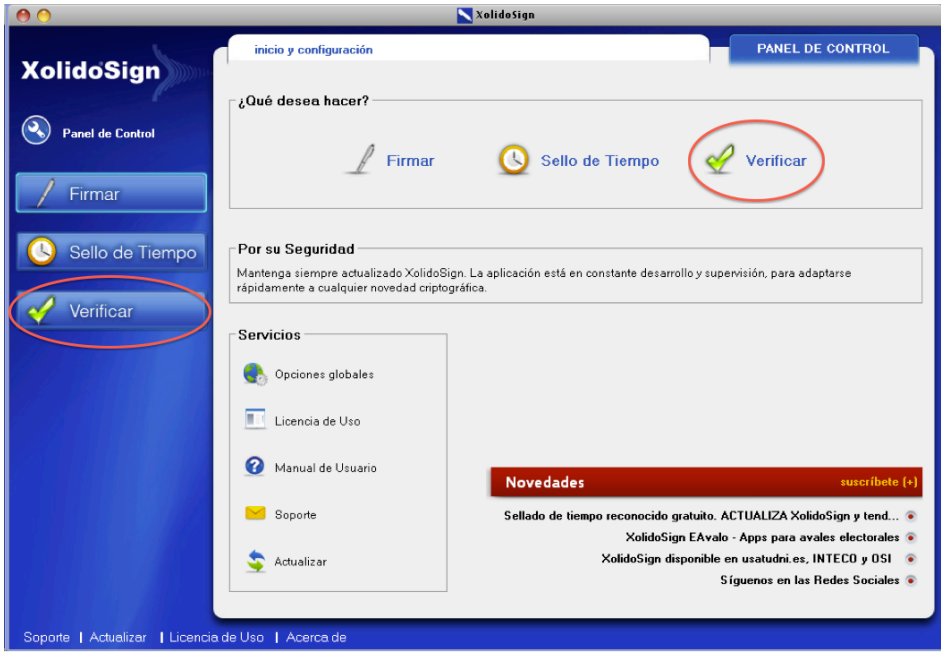


*Figura 7 Ventana de inicio de XolidoSign*

2. Seleccionar “verificación manual”. Mediante los botones “seleccionar archivo” y “seleccionar firmas” se proporcionan a la aplicación los archivos del documento electrónico original (`original.pdf`) y de la firma electrónica (`firma.p7s`). Finalmente pulse “iniciar operación”.

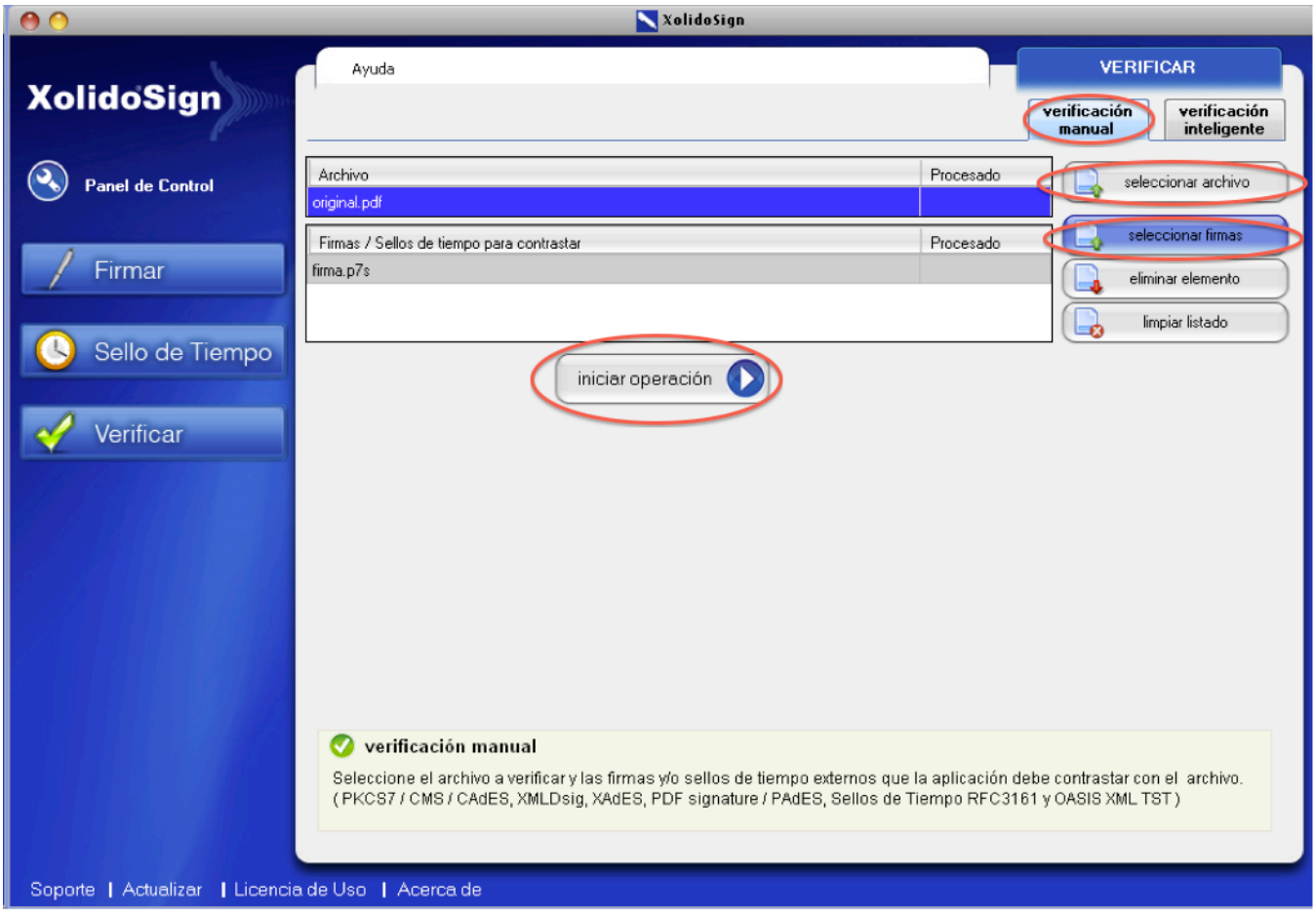


*Figura 8 Selección de los archivos con el documento original y la firma electrónica para validar*

3. La aplicación presenta el resultado resumido de la verificación. Pulsando "ver informe" se puede acceder a un informe detallado de la operación. Como puede verse, la aplicación tampoco es capaz de determinar el estado de revocación del certificado del firmante.

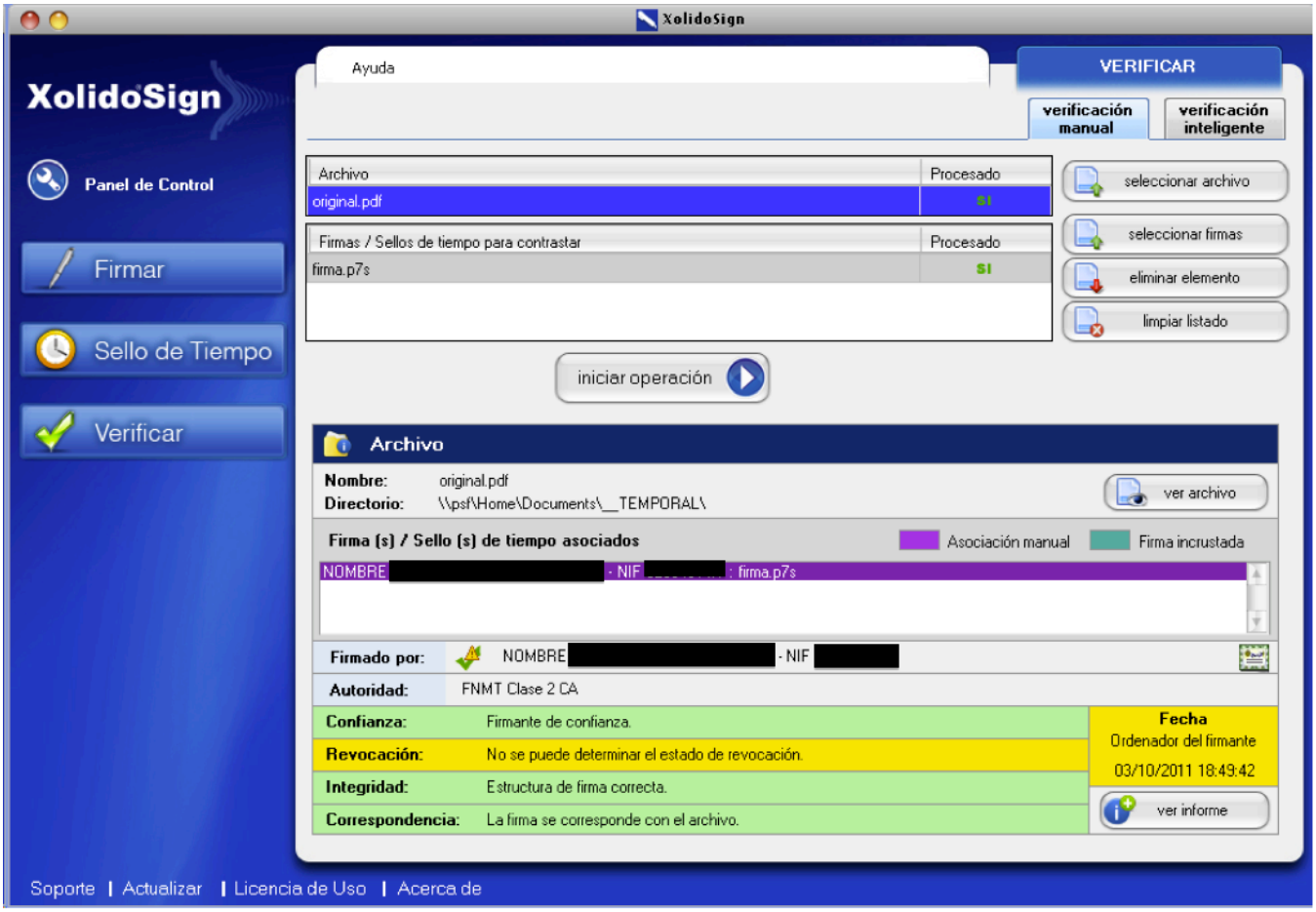


*Figura 9 Resultado de la validación del documento*

# Referencias

1. Verificador de firmas de la Sede Electrónica de la UPM
   https://e-administracion.upm.es/verificadorFirmas

2. Sede Electrónica de la UPM
   https://sede-electronica.upm.es

3. Servicio de validación de firmas electrónicas VALIDe
   https://valide.redsara.es/valide/pages/irValidarFirma

4. Openssl
   http://www.openssl.org

5. XolidoSign
   http://www.xolido.com

6. PKCS#7 (PUBLIC KEY CRYPTOGRAPHY STANDARD #7)
   http://tools.ietf.org/html/rfc2315

7. Copia del estándar ISO 32000 de Adobe
   http://www.adobe.com/devnet/pdf/pdf_reference.html

8. CAPTCHA (Completely Automated Public  Turing Test to Tell Computers and Humans Apart)
   http://es.wikipedia.org/wiki/CAPTCHA