



Banco de la República
Bogotá D. C., Colombia

MANUAL DE INSTALACION Y USO
eSign Viewer

Agosto de 2015



1	OBJETO	3
2	INTRODUCCION	3
3	REQUISITOS DEL SISTEMA	3
4	DESCARGA	4
5	INSTALACIÓN	4
5.1	INSTALACIÓN DESDE EL INSTALADOR DE LA APLICACIÓN	4
5.2	INSTALACIÓN DESATENDIDA	10
6	UN PASO POR ESIGNA® VIEWER	11
6.1	PANTALLA PRINCIPAL	11
6.2	MENÚ ARCHIVO	12
6.3	MENÚ VERIFICACIÓN	14
6.4	MENÚ AYUDA	14
7	VERIFICACIÓN DE DOCUMENTOS FIRMADOS ELECTRÓNICAMENTE	17



1 OBJETO

El presente documento constituye el manual de uso de la aplicación **eSigna® Viewer**.

El objeto de este manual es asistir a todas las personas usuarias en la gestión y uso de la misma.

2 INTRODUCCION

eSigna® Viewer es una aplicación de escritorio que permite visualizar las firmas electrónicas generadas desde sistemas de firma electrónica que cumplen los estándares internacionales, como XAdES, PKCS#7 y firma PDF/PAdES.

También verifica el sellado de tiempo (XAdES, PKCS#7 y firma PDF/PAdES), así como la información del estado de revocación del certificado firmante, incluida en las firmas.

3 REQUISITOS DEL SISTEMA

El equipo en el que vaya a instalar la aplicación **eSigna® Viewer** debe cumplir con unos requisitos mínimos recomendados:

- **Sistemas operativos recomendados:**
 - Microsoft Windows 2000
 - Microsoft Windows XP,
 - Microsoft Windows Vista,
 - Microsoft Windows 7.
- **Hardware:**
 - 512 MB RAM (1 GB RAM recomendados).
 - Un equipo pentium pc o compatible (AMD Athlon).
 - Desde 1 GB de espacio disponible en el disco duro (instalación y funcionamiento).

Muchas de las funcionalidades de eSigna® Viewer, además, necesitan conexión a la red Internet (verificación de certificados, actualización, etc)



4 DESCARGA

<http://datos.indenova.com/download/eSignaViewer/eSignaViewer.exe>

5 INSTALACIÓN

El proceso de instalación de la aplicación de escritorio eSigna® Viewer se podrá llevar a cabo de dos formas diferentes:

5.1 INSTALACIÓN DESDE EL INSTALADOR DE LA APLICACIÓN

Para proceder a la instalación de **eSigna® Viewer**, pulsar sobre el instalador de la aplicación  eSignaViewer_2.3.X_windows.exe. Se mostrará la ventana de selección de idioma, pudiendo escoger entre Castellano, Catalán o Inglés:



Una vez elegido el idioma de la aplicación, se pulsará  y este será el idioma por defecto durante la instalación.

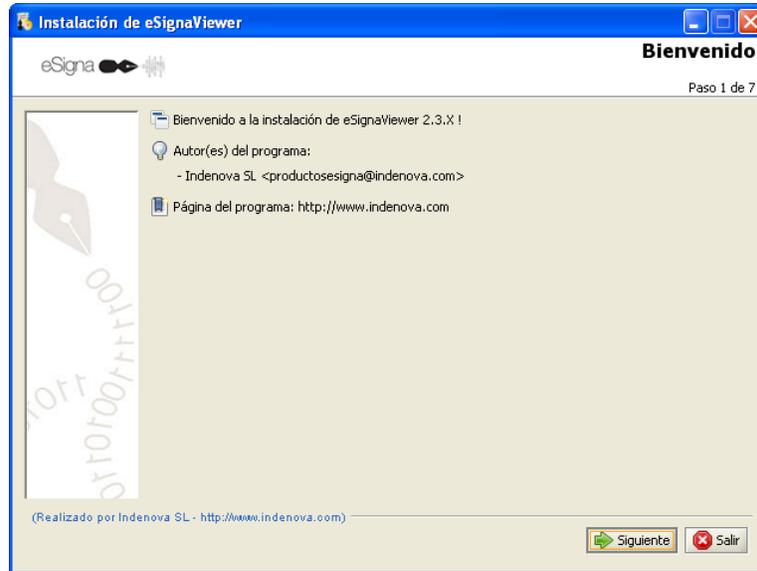
A continuación se mostrará un asistente que le guiará durante la instalación de la aplicación. Desde todas las ventanas tendrá la posibilidad de cancelar la instalación pulsando



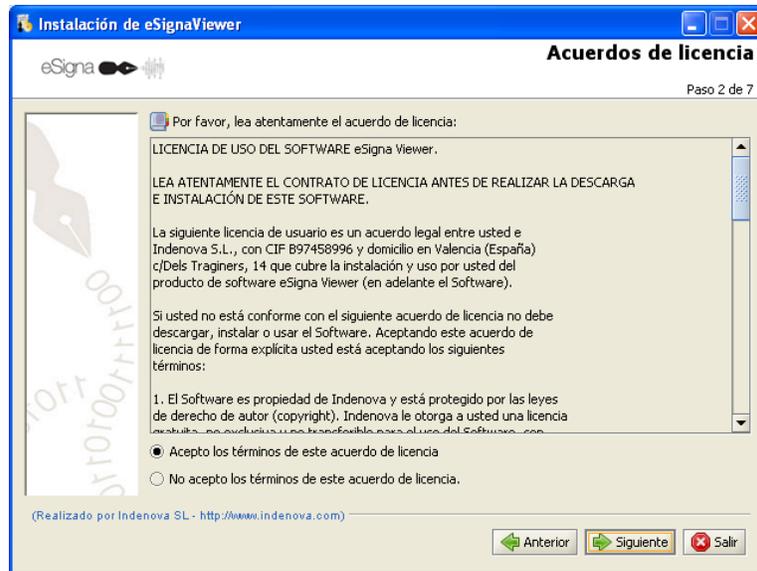
o de volver a la pantalla anterior pulsando



En la siguiente ventana se inicia el asistente de instalación:



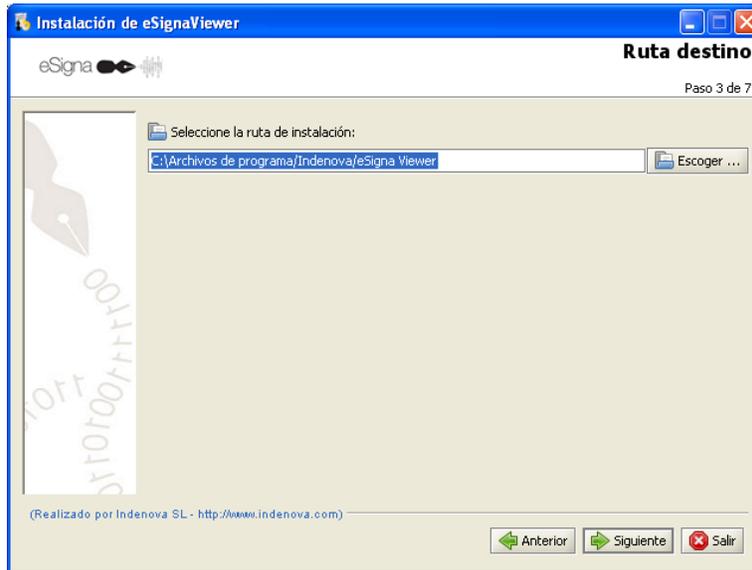
Tras pulsar el botón  se mostrará la siguiente ventana, donde aparecen redactados los términos de la licencia.



Para poder acceder a la siguiente pantalla de instalación deberá marcar la opción **Acepto los términos de este acuerdo de licencia**, aceptando los términos de la licencia, y pulsar el botón .

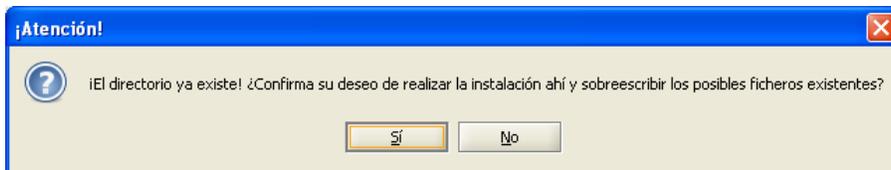


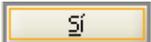
En la siguiente pantalla deberá seleccionar el directorio de instalación de la aplicación, para ello pulsará .



Para continuar con la instalación deberá pulsar el botón  del asistente.

En caso de que ya exista el directorio, aparecerá el siguiente mensaje:



Se pulsará  para continuar, o por el contrario, se pulsará  para volver atrás y cambiar la ruta de instalación.

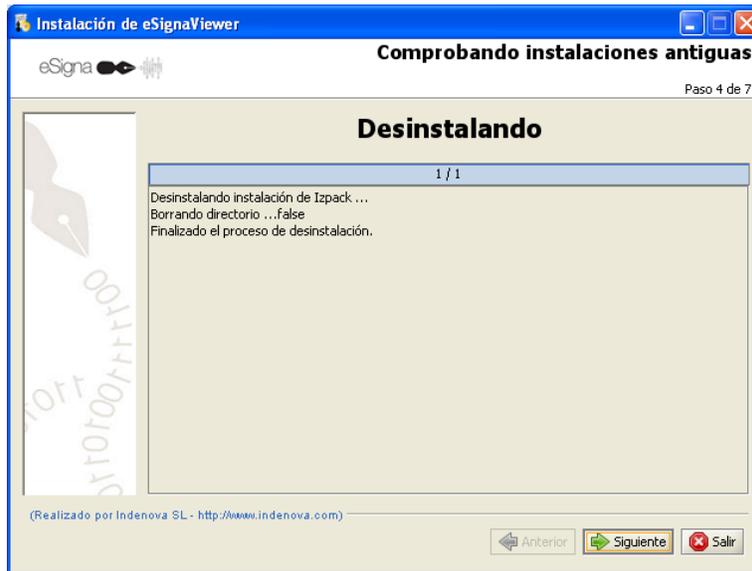
En caso de que el directorio no exista, aparecerá el siguiente mensaje:

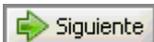




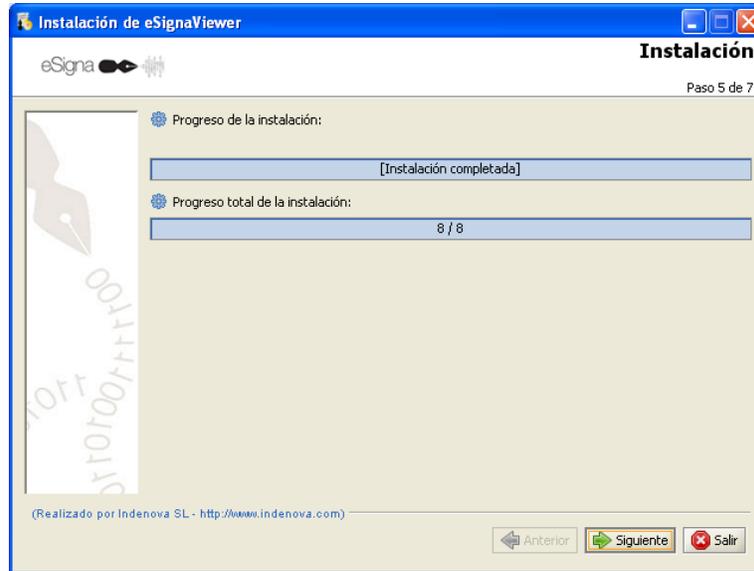
Si se pulsa  se creará el directorio destino de la instalación, en caso contrario, se pulsará .

En caso de tener instalada una versión más antigua de la aplicación, el asistente de instalación comprobará las versiones antiguas e iniciará automáticamente el proceso de desinstalación, la pantalla a mostrar será la siguiente:



Una vez finalizado el proceso de desinstalación, se pulsará  para continuar con el asistente.

Tras ello empezará la instalación de los componentes de la aplicación, mostrando la barra de progreso e indicando el estado de la misma en todo momento.



Una vez instalados los componentes, se pulsará  para continuar con el asistente.

En la siguiente ventana deberá seleccionar la carpeta del menú de inicio desde donde se accederá a la aplicación.





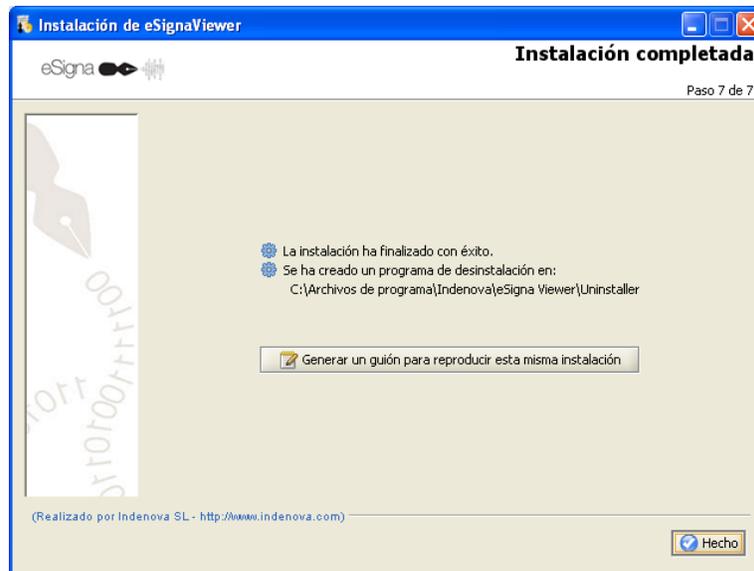
También se podrá configurar si se desea, los accesos directos para la aplicación, para ello deberá marcar las siguientes opciones:

- Crear accesos directos en el menú Inicio : se creará el acceso directo en el menú de inicio.
- Crear accesos directos adicionales en el escritorio : se creará el acceso directo en el escritorio.

Si se desea, se podrá seleccionar el grupo de programas donde se ubicará la aplicación.

También se podrá configurar el acceso directo de la aplicación para el usuario actual o para todos los usuarios, si se desea.

A continuación se pulsará  para continuar con el asistente.



Completada la instalación de los componentes de la aplicación, aparecerá un resumen de la instalación.

También se podrá generar un guión de instalación, de manera que ésta quede automatizada con las opciones seleccionadas durante la instalación actual, para ello se pulsará

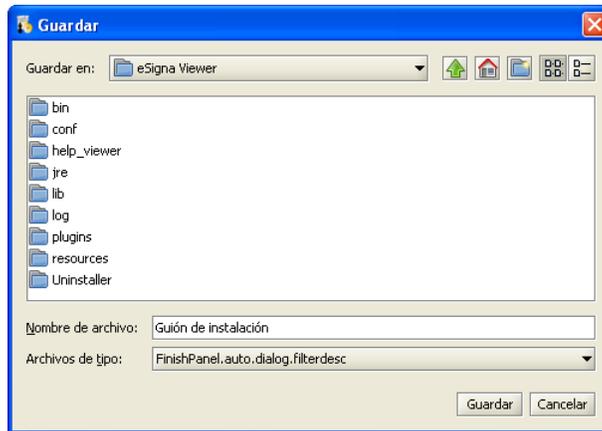


Para completar la instalación, se pulsará .

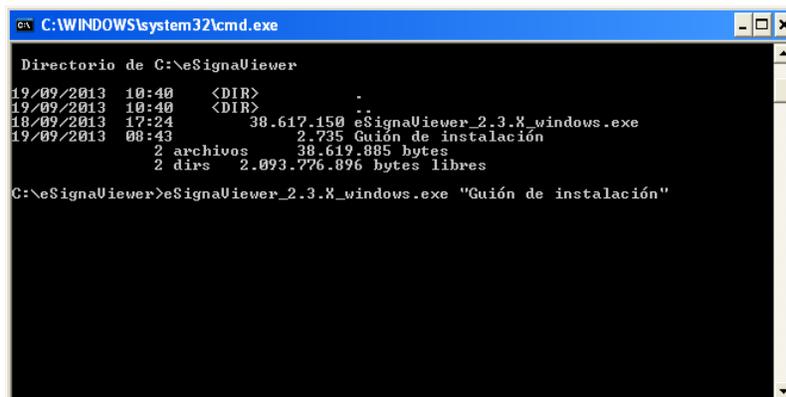
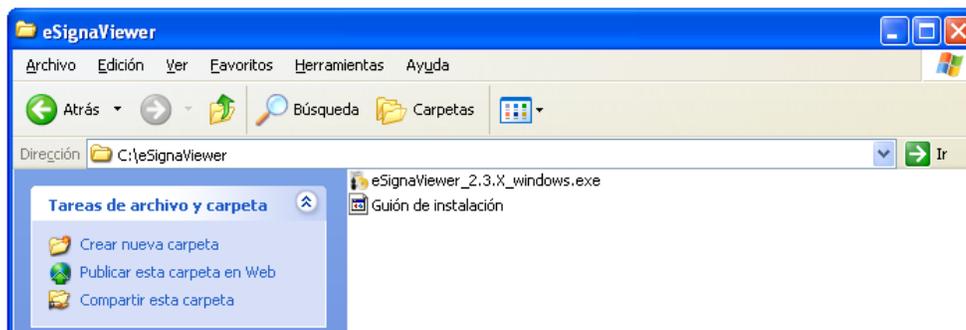


5.2 INSTALACIÓN DESATENDIDA

Para realizar una instalación desatendida, deberá disponer de un guión de instalación previamente generado mediante la opción  Generar un guión para reproducir esta misma instalación, una vez pulsado el botón, la aplicación le pedirá en qué ubicación guardar el guión de instalación.



Una vez se dispone del guión de instalación junto con el instalador de eSigna® Viewer, se podrá realizar la instalación desatendida desde una consola:





Nota: el guión de instalación deberá estar ubicado en el mismo directorio donde se encuentra el fichero ejecutable del eSigna® Viewer.

6 UN PASO POR ESIGNA® VIEWER

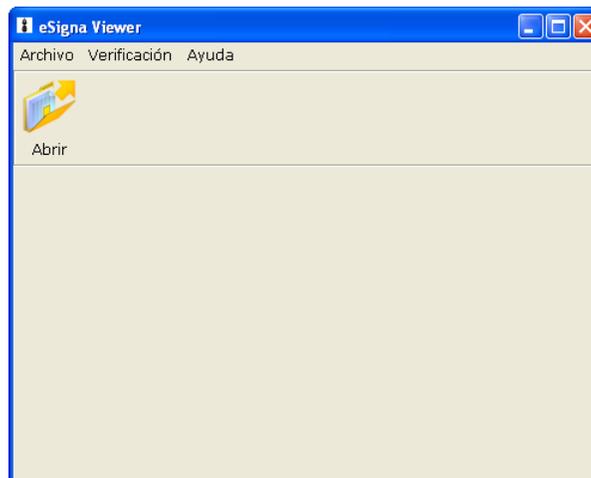
6.1 PANTALLA PRINCIPAL

Para abrir **eSigna® Viewer** habrá varias posibilidades, según se haya configurado durante la instalación:

- Pulsando el icono de acceso directo creado en el escritorio (configurado mediante la opción).
- Pulsando sobre el icono de acceso rápido creado en el menú (configurado mediante la opción **Crear accesos directos adicionales en el escritorio**).

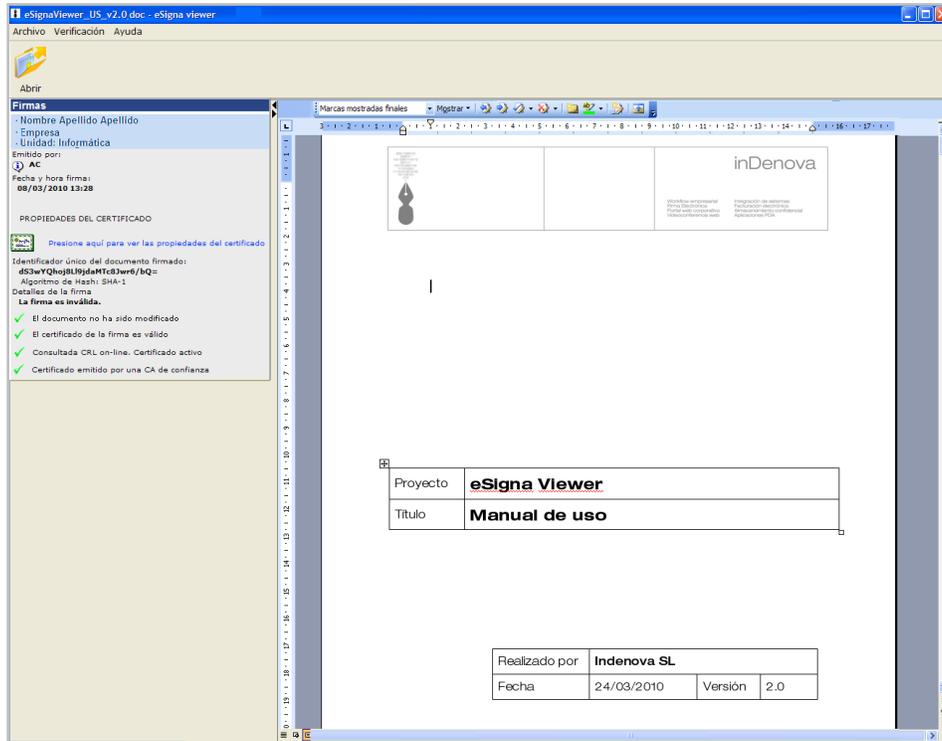


Tras abrir la aplicación **eSigna® Viewer** se mostrará la pantalla principal:



Cuando se seleccione algún documento, la pantalla se dividirá en dos paneles:

- **Panel derecho:** donde se visualizan los documentos.
- **Panel izquierdo:** donde se visualiza el resultado de la verificación.



En la parte superior dispondrá del menú principal y de la barra de herramientas.

Desde esta vista, en la barra de herramientas, tendrá disponible el siguiente botón:



- **Abrir**: permite seleccionar un documento y abrirlo dentro de la aplicación para poder llevar a cabo la verificación de la firma del mismo.

Además dispondrá en la parte superior de tres menús.

6.2 MENÚ ARCHIVO

Desde el menú **Archivo** se podrá abrir, imprimir o cerrar los documentos electrónicos manejados por la aplicación.



Desde este menú estarán disponibles las siguientes opciones:

-  **Abrir archivo**: mediante esta opción se puede abrir cualquier documento electrónico de dos formas diferentes:
 - pulsando sobre la opción  **Abrir archivo ... Ctrl+O**.
 - tecleando la combinación de teclas que se muestra en la opción **Abrir**: **CTRL+O**

Además siempre tendrá disponible desde la barra de herramientas el botón:



Tras pulsar **Abrir**, se mostrará el directorio del equipo informático en el que está instalada la aplicación **eSigna® Viewer**, para seleccionar el documento al que se le desea verificar su firma.

-  **Cerrar**: mediante ésta opción se podrá cerrar el documento electrónico que se encuentre abierto en la aplicación.
-  **Imprimir**: se podrá imprimir el documento electrónico seleccionado de dos formas diferentes:
 - pulsando sobre la opción  **Imprimir** **Ctrl+P**.
 - tecleando la combinación de teclas que se muestra junto a la opción: **CTRL+P**
-  **Salir**: mediante ésta opción se podrá salir de la aplicación.



6.3 MENÚ VERIFICACIÓN

Desde el menú **Verificación** se pueden verificar el contenido y las firmas de los documentos electrónicos manejados por la aplicación.

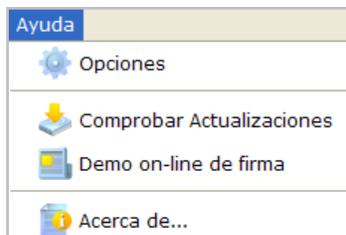


Desde este menú estarán disponibles las siguientes opciones:

-  **Extraer archivo original ...**: mediante esta opción se puede recuperar el archivo en el estado en que se encontraba antes de aplicarle la firma, para realizar modificaciones. No se podrá modificar un documento firmado. Un documento modificado después de ser firmado digitalmente, perderá toda su validez legal.
-  **Generar códigos PDF-417**: esta opción permite generar los códigos de barras en formato PDF417 con el contenido del documento y las firmas aplicadas a él.
-  **Verificar certificado**: esta opción permite comprobar la validez y estado del certificado digital con el que se firmó el documento.
-  **Recargar**: mediante esta opción se vuelve al estado de verificación de la firma.

6.4 MENÚ AYUDA

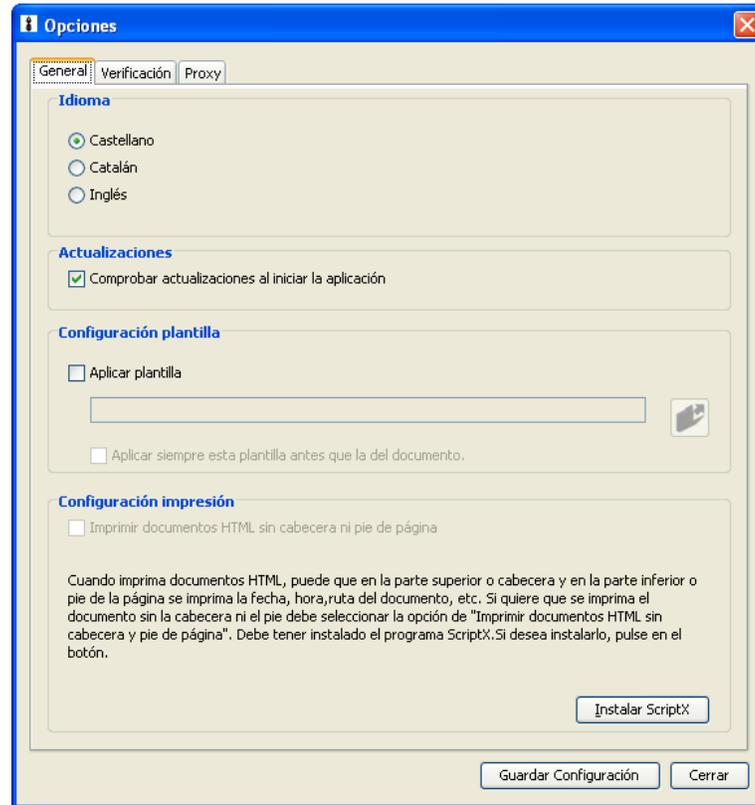
Desde el menú **Ayuda** se podrá consultar cualquier tema relacionado con la aplicación.



Desde este menú estarán disponibles las siguientes opciones:



-  **Opciones** : mostrará una vista como la siguiente desde la que podrá configurar las siguientes opciones:



Desde la pestaña **General** se podrán configurar las siguientes opciones:

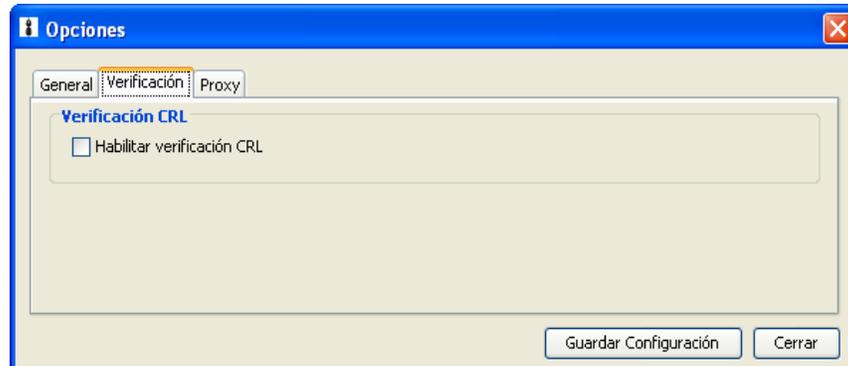
- **Idioma:** mediante ésta opción se puede seleccionar el idioma de la aplicación.
- **Actualizaciones:** si desea que al acceder a la aplicación se compruebe si hay alguna actualización disponible, se marcará la opción Comprobar actualizaciones al iniciar la aplicación .
- **Configuración plantilla:** si desea aplicar una plantilla a un documento xml (factura o trámite) siempre que el documento no contenga una plantilla), se marcará la opción Aplicar plantilla y se pulsará  para ubicar la plantilla.
Si se desea que se aplique siempre la plantilla a cualquier documento xml, se marcará la opción Aplicar siempre esta plantilla antes que la del documento .
- **Configuración impresión:** si desea que la impresión de los documentos electrónicos no lleve ninguna cabecera ni pie de página, se marcará la opción Imprimir documentos HTML sin cabecera ni pie de página . Para poder seleccionar esta opción debe tener instalado el programa ScriptX. Si no



dispone del mismo podrá llevar a cabo la instalación pulsando

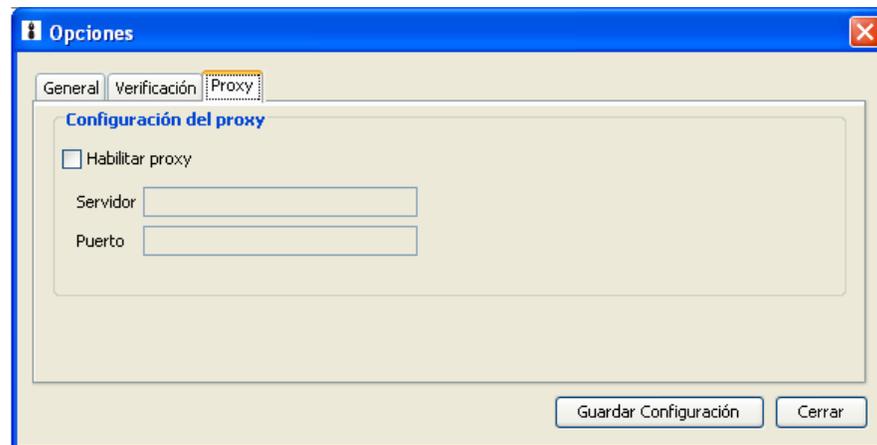
[Instalar ScriptX](#)

La pestaña **Verificación** permite configurar las siguientes opciones:



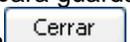
- **Verificación CRL:** si la opción **Habilitar verificación CRL** se encuentra habilitada, comprueba el estado del certificado.

La pestaña **Proxy** permite configurar las siguientes opciones:



- **Configuración del proxy:** si se trabaja con un servidor Proxy, se introducirá el servidor y puerto correspondientes para poder realizar la conexión al servidor correctamente.



Desde cualquiera de las pestañas se podrá pulsar  para guardar los cambios llevados a cabo. Si no se desea guardar las opciones marcadas se pulsará .

-  **Comprobar Actualizaciones** : permite buscar por internet si existen actualizaciones disponibles para instalar.
-  **Demo on-line de firma** : al pulsar sobre ésta opción, se abrirá un enlace a una página de demostración sobre firma electrónica.
-  **Acerca de...** : permite consultar información sobre la aplicación.

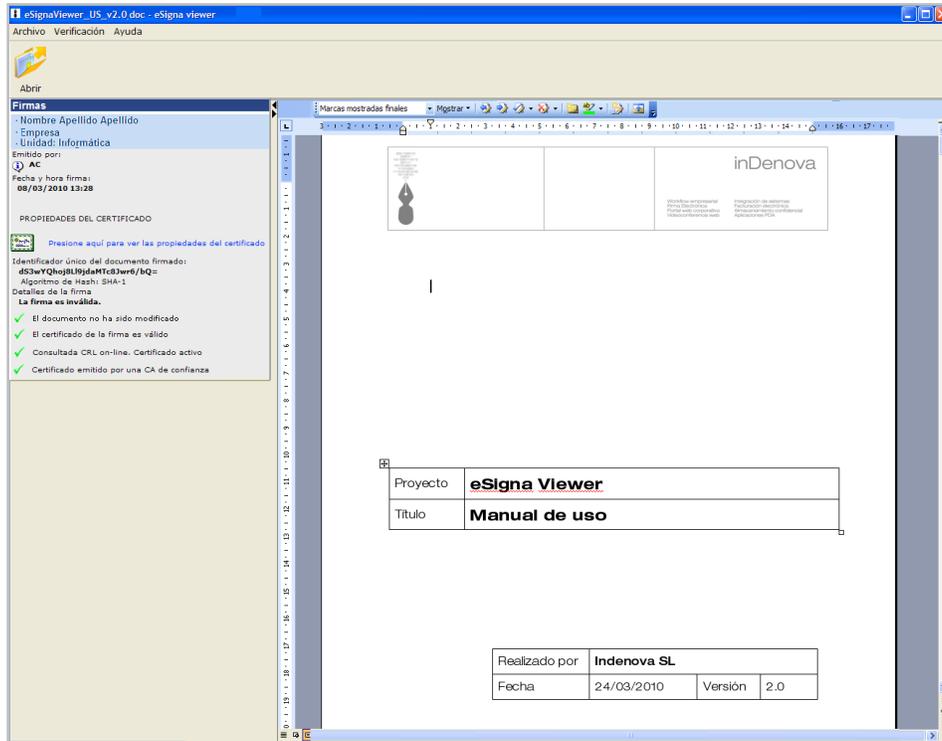


7 VERIFICACIÓN DE DOCUMENTOS FIRMADOS ELECTRÓNICAMENTE

Podrá verificar cualquier tipo de documento firmado con los formatos de firma más utilizados como: XAdES, PKCS#7, y firma PDF/PAdES.

También se podrá verificar el sellado de tiempo (XAdES, PKCS#7, y firma PDF/PAdES), así como la información de estado de revocación del certificado firmante incluida en las firmas (XAdES).

Esta información se mostrará en el panel izquierdo al abrir cualquier documento firmado (.esig, .xml o .pdf).



Una vez abierto el documento firmado, la aplicación mostrará el resultado de la verificación (con tantos paneles de verificación como firmas tenga el documento) en la parte izquierda de la aplicación y el documento original firmado en la parte derecha.

A continuación se detalla el panel de verificación de una firma y los diferentes casos de verificación que se pueden llegar a dar:



Firmas

. NOMBRE APELLIDO APELLIDO
. EMPRESA
. Unidad: SECRETARIA

Emitido por:
i RACER

PROPIEDADES DEL CERTIFICADO

[Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=

Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

De cada una de las firmas aplicadas a un documento se mostrará la siguiente información:

- **Datos del firmante:** se mostrarán, en la parte superior del recuadro, los datos del firmante junto con el nombre de la empresa y unidad a las que pertenece (en el caso de certificado de pertenencia a empresa).

Firmas

. NOMBRE APELLIDO APELLIDO
. EMPRESA
. Unidad: SECRETARIA

Emitido por:
i RACER

PROPIEDADES DEL CERTIFICADO

[Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=

Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

- **Autoridad de Certificación:** mostrará la Autoridad de Certificación emisora del certificado del firmante.



Firmas

· NOMBRE APELLIDO APELLIDO
· EMPRESA
· Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

 [Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=
Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

- **Propiedades del certificado:** se podrán visualizar las propiedades del certificado del firmante.

Firmas

· NOMBRE APELLIDO APELLIDO
· EMPRESA
· Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

 [Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

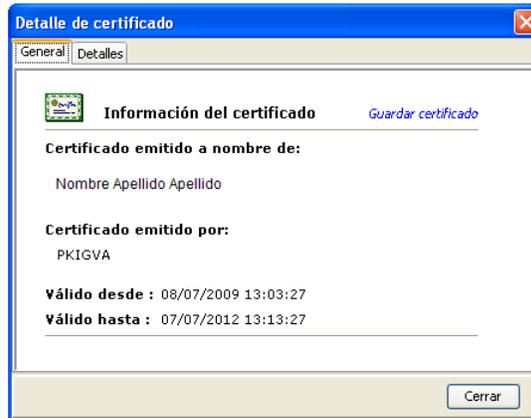
FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=
Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

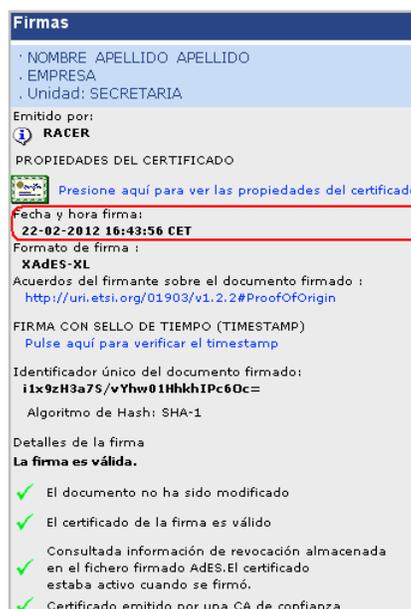
- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

Pulsando en el enlace [Presione aquí para ver las propiedades del certificado](#), aparecerá una ventana con los detalles del certificado.



Desde esta ventana, la información se mostrará en dos pestañas:

- Pestaña **General**: aparecerá el nombre del titular del certificado, la autoridad de certificación y el periodo de validez del mismo. Además, si se pulsa en el enlace [Guardar certificado](#) se podrá almacenar el certificado de la firma en formato DER (.crt), este certificado es la parte pública que contiene la información necesaria para verificar el fichero firmado (datos del firmante).
 - Pestaña **Detalles**: se podrán visualizar otras propiedades del certificado, como los usos del mismo, puntos de distribución de información de revocación, emisor, titular, etc.
- **Fecha y hora firma**: mostrará la fecha y hora en que se realizó la firma.





- **Formato de firma:** mostrará el tipo de firma aplicada y el perfil. Su formato será *tipo-perfil*.

Firmas

. NOMBRE APELLIDO APELLIDO
. EMPRESA
. Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

[Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=
Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

En caso de tratarse de una firma PAdES, el formato de la segunda firma se tratará de una marca de hora (sellado de tiempo).

Firmas

. NOMBRE APELLIDO APELLIDO
. EMPRESA
. Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

[Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 14:02:31 CET

Formato de firma :
Firma de marca de hora del documento.

Identificador único del documento firmado:
3nikHwI7Bl1WEpTYrE3AH00wa8=
Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada CRL on-line. Certificado activo
- ✓ Certificado emitido por una CA de confianza

- **Acuerdos del firmante sobre el documento firmado:** en el caso de que la firma contenga unos acuerdos o diligencias del firmante, estos se mostrarán tras el formato de la firma.



Firmas

· NOMBRE APELLIDO APELLIDO
· EMPRESA
· Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

Presione aquí para ver las propiedades del certificado

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=
Algoritmo de Hash: SHA-1

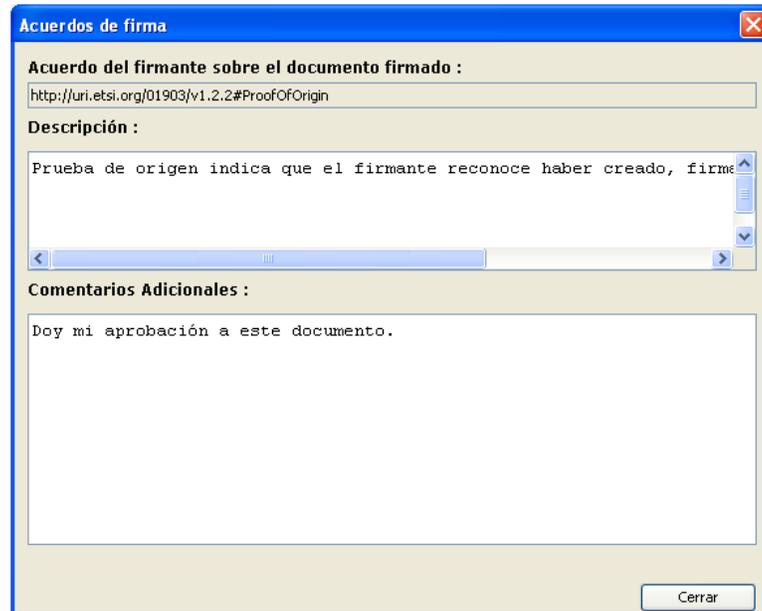
Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES.El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

Podrá consultar los acuerdos o diligencias del firmante pulsando en los siguientes tipos de enlaces:

- <http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>
- <http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt>
- <http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery>
- <http://uri.etsi.org/01903/v1.2.2#ProofOfSender>
- <http://uri.etsi.org/01903/v1.2.2#ProofOfApproval>
- <http://uri.etsi.org/01903/v1.2.2#ProofOfCreation>

La información se le mostrará en una ventana como la siguiente, y en función del tipo de enlace seleccionado aparecerá una descripción u otra.



Si el tipo de enlace termina con alguna de las siguientes palabras, las descripciones serán las siguientes:

- **Proof of origin:** “Prueba de origen indica que el firmante reconoce haber creado, firmado y enviado el documento firmado”.
- **Proof of receipt:** “Prueba de recepción indica que el firmante reconoce haber recibido el contenido del documento firmado”.
- **Proof of delivery:** “Prueba de entrega indica que la entidad (TSP) que provee la indicación ha entregado el documento firmado en un almacén local accesible por el receptor del documento firmado”.
- **Proof of sender:** “Prueba de envío indica que el firmante ha enviado el documento firmado (pero no lo ha creado necesariamente)”.
- **Proof of approval:** “Prueba de aprobación indica que el firmante aprueba el contenido del documento firmado”.
- **Proof of creation:** “Prueba de creación indica que el firmante ha creado el documento firmado (pero no lo ha aprobado necesariamente o no lo envió)”.

También aparecerán los comentarios adicionales de la persona usuaria que ha firmado el documento.

- **Sellado de tiempo:** en el caso de que la firma contenga un sello de tiempo, éste se mostrará tras la información de la Autoridad de Certificación.



Firmas

. NOMBRE APELLIDO APELLIDO
. EMPRESA
. Unidad: SECRETARIA

Emitido por:
i RACER

PROPIEDADES DEL CERTIFICADO

[Presione aquí para ver las propiedades del certificado](#)

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HkhIPc60c=

Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES. El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

Podrá verificar este sellado pulsando en el enlace [Pulse aquí para verificar el timestamp](#). La información se le mostrará en una ventana como la siguiente:

Sello de tiempo (Time Stamp)

Información del sello de tiempo

Algoritmo de Hash	Hash al que se le aplicó el sello de tiempo
SHA-1 (OID: 1.3.14.3.2.26)	OxhYFtBJig78bS0pmuhI2OqD1w4=

Se ha verificado que el sello de tiempo fue aplicado a esta firma electrónica. Por tanto, la firma y los datos firmados quedan garantizados en la fecha indicada por la autoridad de certificación

Fecha y hora del sello de tiempo
22/02/2012 16:43:51

Autoridad de certificación
Root CA Generalitat Valenciana

En esta ventana se mostrará el tipo de algoritmo empleado y el valor resumen (Hash), el resultado de la verificación del sello de tiempo, la fecha en la que se emitió el sello de tiempo y la autoridad de sellado.

- **Resultado de la firma:** mostrará los detalles del resultado de la verificación de la firma.



Firmas

· NOMBRE APELLIDO APELLIDO
· EMPRESA
· Unidad: SECRETARIA

Emitido por:
RACER

PROPIEDADES DEL CERTIFICADO

Presione aquí para ver las propiedades del certificado

Fecha y hora firma:
22-02-2012 16:43:56 CET

Formato de firma :
XAdES-XL

Acuerdos del firmante sobre el documento firmado :
<http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin>

FIRMA CON SELLO DE TIEMPO (TIMESTAMP)
[Pulse aquí para verificar el timestamp](#)

Identificador único del documento firmado:
i1x9zH3a7S/vYhw01HhkhIPc60c=
Algoritmo de Hash: SHA-1

Detalles de la firma
La firma es válida.

- ✓ El documento no ha sido modificado
- ✓ El certificado de la firma es válido
- ✓ Consultada información de revocación almacenada en el fichero firmado AdES. El certificado estaba activo cuando se firmó.
- ✓ Certificado emitido por una CA de confianza

Donde se detalla el resumen (Hash) del valor de la firma (que comprende el resumen del fichero y otros resúmenes como el del certificado), el algoritmo para el cálculo del resumen (Hash) y los detalles del resultado de verificación de la firma (puede ser válida, inválida o parcialmente válida).

- **Integridad del documento:** indica si el documento firmado electrónicamente ha sido modificado o no. Si el resultado aparece con el icono ✓, significa que no ha sido modificado, con lo cual, el identificador que aparece en el panel coincide con el identificador calculado en el proceso de verificación. Si el resultado aparece con el icono ✗, significa que el documento original que se firmó no coincide con el documento que se acaba de abrir y verificar.
- **Validez del certificado:** implica que el certificado era vigente en el momento en que se realizó la firma, aparecerá el icono ✓. Si el certificado está expirado en la actualidad y se desconoce si era válido en el momento en que se aplicó la firma (no lleva sello de tiempo o la fecha no proviene de una fuente fiable), aparecerá el icono !. En el caso que el documento se firme con un certificado no válido (caducado), aparecerá el icono ✗.
- **Estado del certificado:** indica el estado del certificado actual respecto a la fecha de firma y el método que se ha empleado para comprobar dicho estado (CRL, OCSP o LDAP), si el estado es correcto aparecerá el icono ✓. En caso de no poder comprobar el estado del certificado, o se desconoce si el certificado estaba activo en el momento en que se aplicó la firma (no lleva sello de tiempo o la fecha no proviene de una fuente fiable), aparecerá el



icono . En caso de que el documento se firme con un certificado revocado, aparecerá el icono .

- **Confianza en la Autoridad de Certificación:** indica si la Autoridad de Certificación emisora del certificado firmante es de confianza , o no . En esta versión las Autoridades de Certificación de confianza que están predeterminadas son:

- AC ABOGACÍA
- ANCERT – Agencia Notarial de Certificación
- ANF AC
- Autoritat de Certificació de la Comunitat Valenciana – ACCV
- Banesto CA
- Camerfirma, Camerfirma/RACER
- CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)
- CICCOP
- Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía – DNIE
- EDICOM
- Entidad de Certificación de la Organización Médica Colegial (EC- OMC)
- Firmaprofesional, S.A.
- Gerencia de Informática de la Seguridad Social
- HEALTHSIGN, S.L.
- Izenpe, S.A.
- Ministerio de Defensa de España
- Ministerio de Trabajo e Inmigración
- Registradores De España