

Xolido®Sign Desktop

V2.2.1.X
Manual de usuario

XOLIDO

firma electrónica, notificaciones y envío seguro de documentos



ÍNDICE

1. Introducción.....	3
2. Xolido®Sign - Panel de Control.....	5
3. Uso de la aplicación Xolido®Sign - Firmar.....	12
3.1. Zona de Gestión de Documentos.....	13
3.2. Zona de Gestión de Certificados Electrónicos.....	14
3.3. Zona de Gestión de la Carpeta de Salida.....	15
3.4. Zona de Gestión de las Opciones de Operación.....	16
3.5. Zona de Inicio de Operación.....	18
4. Uso de la aplicación Xolido®Sign – Sello de tiempo.....	19
4.1. Zona de Gestión de Documentos.....	20
4.2. Zona de Gestión de Servidor de Sello de Tiempo.....	21
4.3. Zona de Gestión de la Carpeta de Salida.....	21
4.4. Zona de Opciones de Operación.....	22
4.5. Zona de Inicio de Operación.....	23
5. Guía de Configuración de Xolido®Sign – Firmar y Sello de Tiempo.....	24
5.1. Zona de Opciones de Certificados.....	25
5.2. Zona de Opciones de Firma.....	28
5.3. Zona de Sello de Tiempo.....	34
5.4. Zona de Opciones de PDF.....	36
5.5. Zona de Opciones de Salida.....	40
5.6. Zona de Opciones Avanzadas.....	43
6. Uso de la aplicación Xolido®Sign - Verificar.....	47
6.1. Modos de verificación.....	47
6.2. Proceso de verificación electrónica.....	50
6.3. Resultados de verificación.....	53
7. Información técnica adicional de Xolido®Sign.....	59
8. Otra información acerca de Xolido®Sign.....	60

1. Introducción



En esta guía se describe paso a paso el procedimiento de uso de la **aplicación gratuita Xolido® Sign** disponible para plataforma Windows proporcionada por Xolido Systems para la firma digital, sellado de tiempo y verificación electrónica de documentos firmados, firmas y sellos de tiempo.

Xolido® Sign le permite realizar en su ordenador, de una manera sencilla e intuitiva, la firma electrónica de todos aquellos documentos que usted desee. Xolido® Sign también permite aplicar sello de tiempo digital a sus documentos, tanto independiente como incrustado en las firmas digitales, usando para ello un servidor compatible RFC 3161 que usted determine.

Durante el proceso, la aplicación tiene en cuenta las medidas de control y seguridad apropiadas, como chequeos de revocación de los certificados, comprobación de integridad...

Xolido® Sign también permite realizar la verificación de firmas electrónicas, sellos de tiempo y archivos firmados. Soporta firmas externas de archivos de cualquier tipo y extensión, independientemente de su tamaño e incrustadas en documentos PDF, así como verificación de sellados de tiempo. La verificación digital de documentos se realiza siguiendo las correspondientes pautas de control de seguridad y se muestra en todo momento al usuario la información completa con el resultado de cada una de las verificaciones realizadas.

Ambas funcionalidades se llevan a cabo en un proceso automático, sin complicaciones en la forma de uso. Para ello presentan una interfaz sencilla y un estilo auto-explicativo que le irán guiando a lo largo de los procesos de firma y verificación de archivos.

Xolido®Sign está destinada a su uso por parte de cualquier tipo de profesional o ciudadano facilitando el acercamiento de las nuevas tecnologías de firma electrónica, verificación y sellado de tiempo a todo tipo de colectivos, desde estudiantes, ingenieros, profesionales de cualquier índole, PYMES, autónomos, funcionarios...

Empleando esta aplicación, conseguirá simplificar enormemente el proceso de firma y verificación electrónica de sus documentos. También reducirá el tiempo en sus procedimientos documentales y los costes en sus envíos (sellos, sobres, papel...) empleando los archivos electrónicos y pudiendo mantener la seguridad en sus trámites (facturas, contratos, publicación de notas, envío de expedientes...).

2. Xolido®Sign - Panel de Control

Xolido®Sign se inicia por defecto mostrando la interfaz del Panel de Control. Desde ahí el usuario puede gestionar y acceder a las principales características de la aplicación. La imagen a continuación muestra dicho Panel de Control.

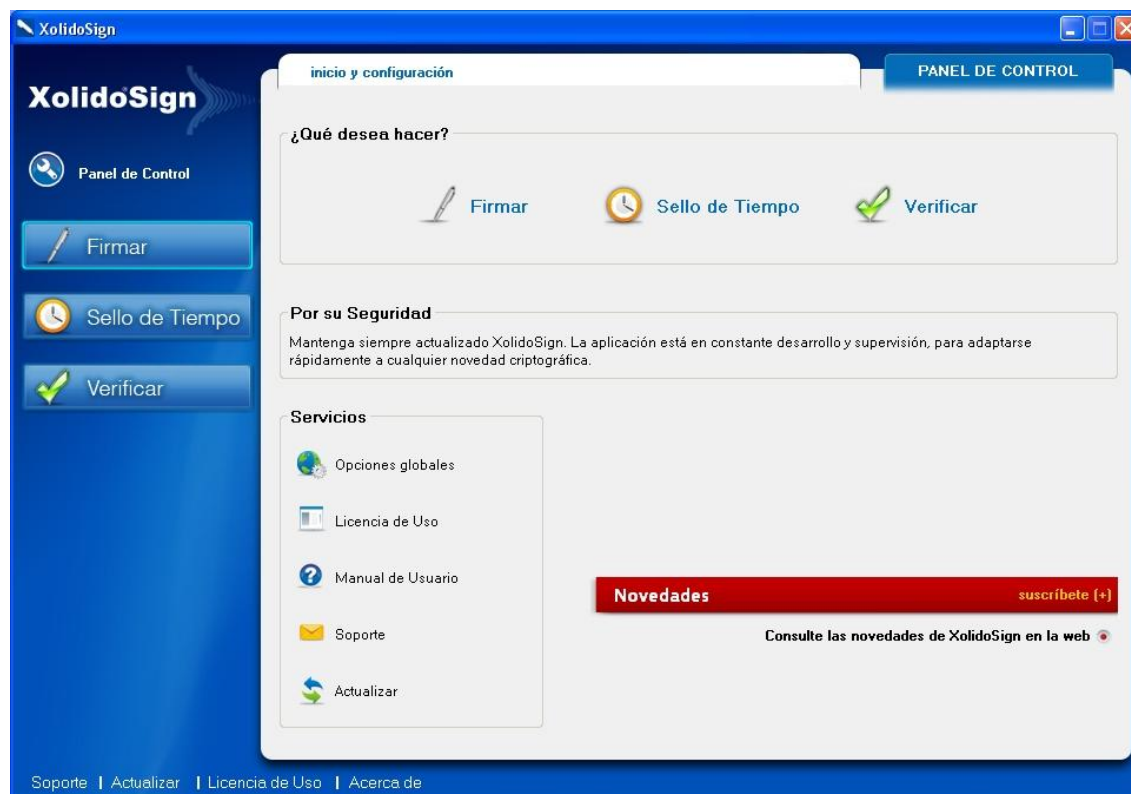


Fig. 1. Panel de Control de Xolido®Sign.

Se presentan en la zona lateral izquierda los botones de acceso directo a las opciones de Firma, Sello de tiempo y Verificación de Xolido®Sign. También se podrá acceder a estas funcionalidades a partir de los enlaces de acceso directo enmarcados en la zona titulada “¿Qué desea hacer?”.

El Panel de Control dispone de una sección “Novedades Xolido®Sign”, desde la cual el usuario permanece al día respecto a los posibles avances o mejoras surgidas en el entorno de los servicios criptográficos en general y referentes a la aplicación en particular.

En la zona inferior izquierda se presenta la sección “Servicios”, desde la cual se tiene acceso directo a varias características genéricas de la aplicación.

También se presentan varios accesos directos (*Soporte, Actualizar, Licencia de uso y Acerca de*) en la franja inferior de la aplicación, que permanecen visibles en todo momento, independientemente de la funcionalidad que se esté ejecutando.

Las Opciones globales de configuración de Xolido®Sign hacen referencia a los parámetros genéricos de uso y se presentan a continuación:

- Aplicación de inicio de Xolido®Sign

En esta sección del panel de configuración global se puede **seleccionar la funcionalidad de inicio de la aplicación**. Por defecto el valor en el arranque es el Panel de Control, pero pueden establecerse cualquiera de las opciones Firmar, Sello de Tiempo o Verificar, de modo que la aplicación se iniciará en sus próximas ejecuciones presentando la interfaz del módulo seleccionado directamente.

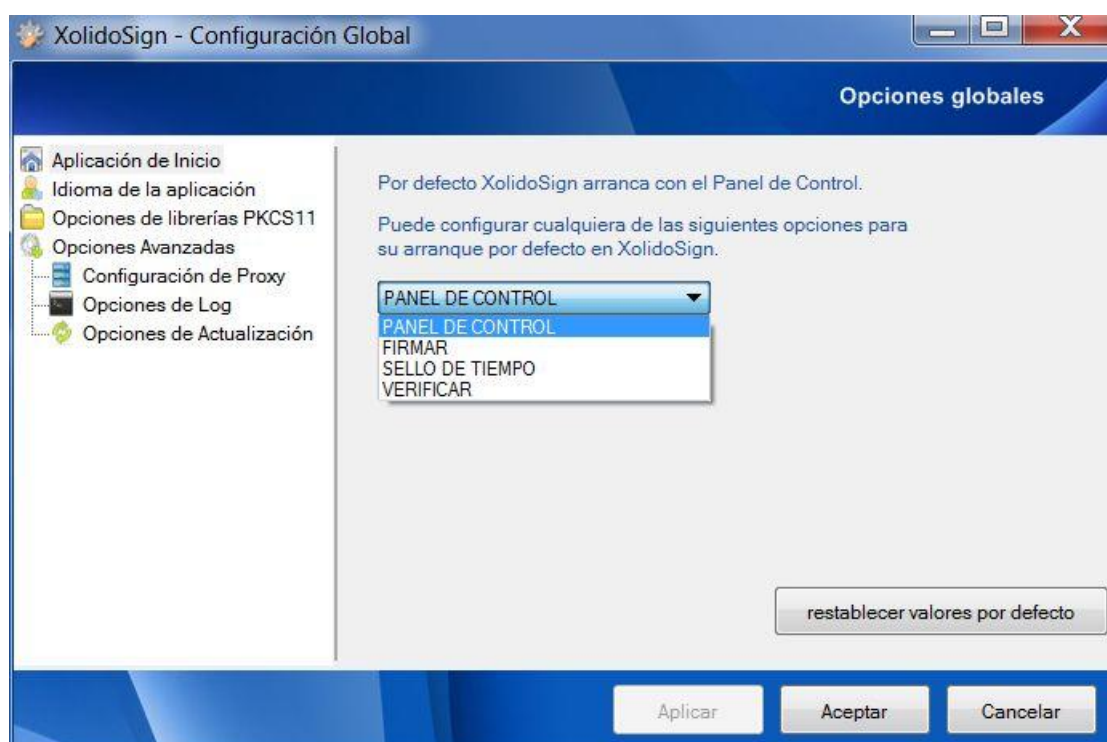


Fig. 2. Configuración de la aplicación de inicio.

- Configuración del idioma de la aplicación

Se deja al usuario la opción de **seleccionar el idioma de trabajo de la aplicación**, por defecto, ésta detecta automáticamente el idioma según la localización declarada en su sistema operativo, no

obstante en la aplicación se deja abierta la posibilidad de predefinir el idioma deseado, cuya entrada en efecto se produce tras reiniciar el programa.

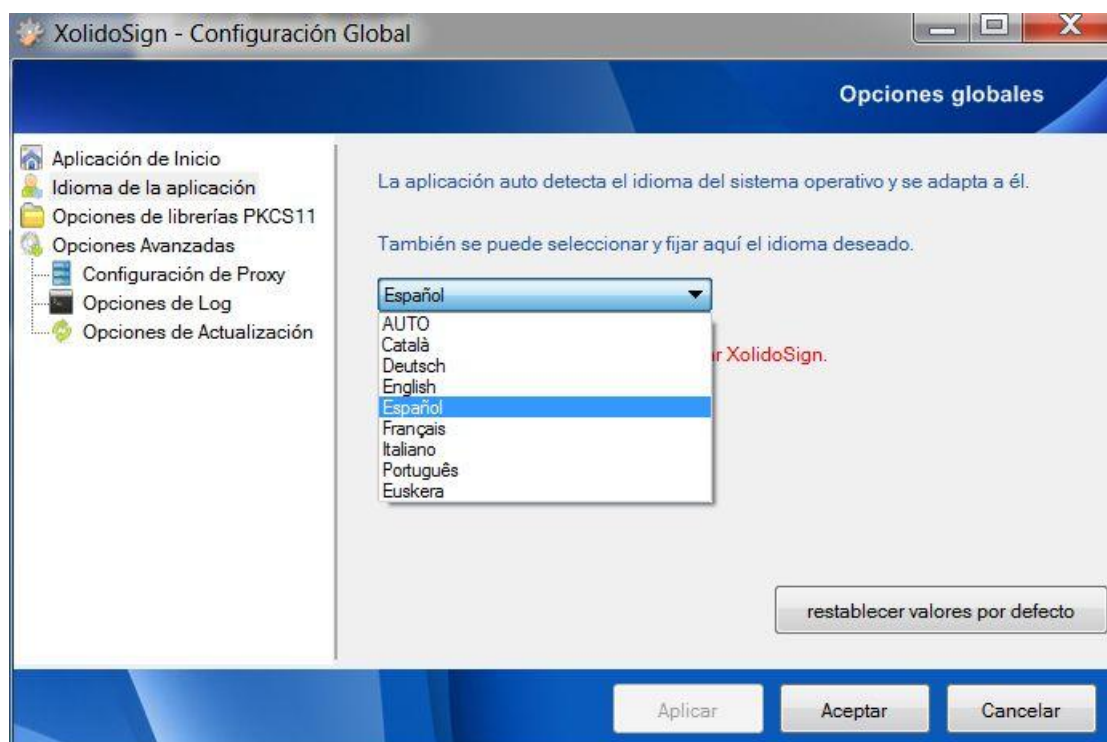


Fig. 3. Configuración del idioma de la aplicación.

- Configuración de las opciones de librerías PKCS11

Xolido®Sign opera por defecto con el almacén de certificados electrónicos del sistema operativo, basándose en los driver CSP que cada fabricante de tarjetas despliega para sus smart card.

Sin embargo, también soporta la posibilidad de acceder a certificados electrónicos de tarjetas criptográficas a través de **librerías PKCS11**, permitiendo al usuario configurar un conjunto de librerías y activar dicha funcionalidad de forma que Xolido®Sign pueda acceder a dichos certificados de manera desatendida.

El usuario introducirá para cada librería que desee añadir y configurar un nombre identificativo y una ruta de acceso a la librería propiamente, para que Xolido®Sign pueda acceder a ella cuando se requiera el uso de certificados electrónicos.

En la figura inferior se muestra la pestaña correspondiente a dicha configuración.

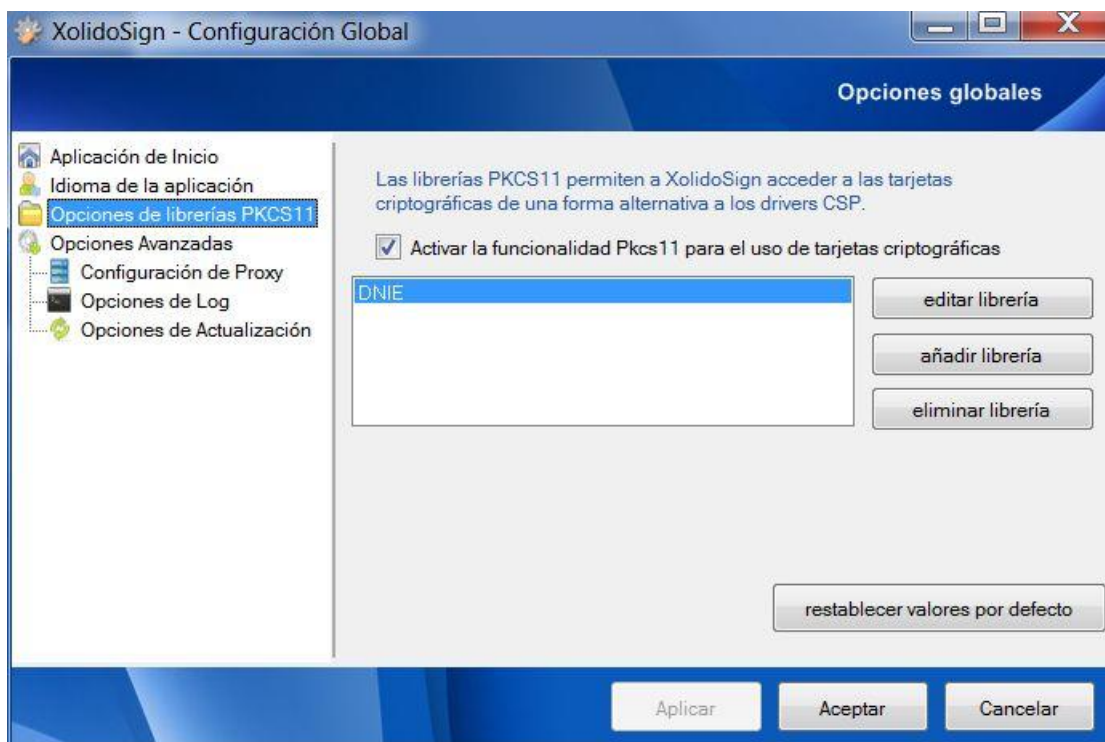


Fig. 4. Configuración de las opciones de librerías PKCS11.

- Configuración de las opciones de Proxy

La aplicación cuenta con funcionalidad para configurar su **conexión a la red a través de servidor Proxy**.

En primer lugar, y si el usuario no indica lo contrario, el programa se conectará al exterior de forma directa, sin servidor proxy intermedio.

El usuario puede establecer que Xolido®Sign utilice un servidor intermedio para el acceso a la red exterior, tomando como referencia la configuración establecida en el navegador Internet Explorer, que el sistema operativo emplea por defecto.

Por otro lado, el usuario también puede especificar una configuración manual para el servidor proxy que desea que utilice Xolido®Sign en su conexión a la red.

En la imagen a continuación se muestra la pestaña donde aparecen las opciones referentes a la configuración de proxy de red para Xolido®Sign.

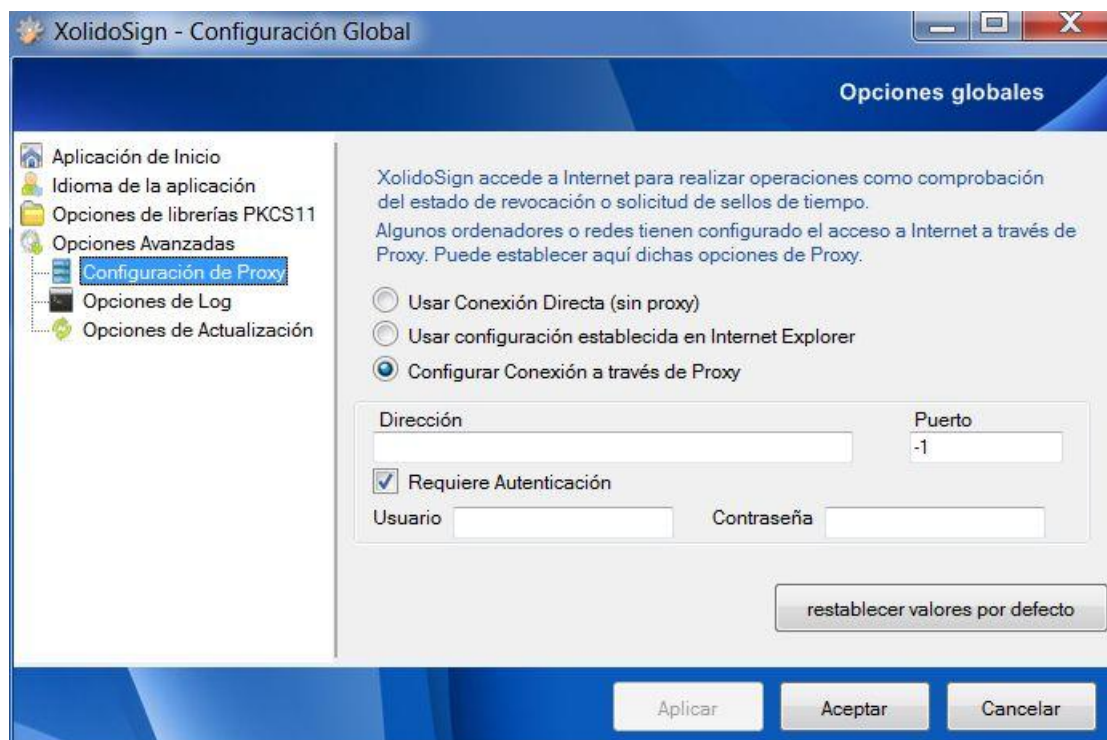


Fig. 5. Configuración de las opciones de servidor Proxy.

- Configuración de las opciones de Log

Se presenta un cuadro de texto en el que se podrá editar a mano la **ruta establecida para el volcado de datos de Log**, en caso de querer llevar a cabo una inspección de incidencias durante la ejecución de la aplicación.

Además, para llevar a cabo dicho volcado de información en el archivo de Log será necesario marcar la opción de **Activar volcado de Log en Archivo Configurado**.

Por defecto esta opción está desactivada.

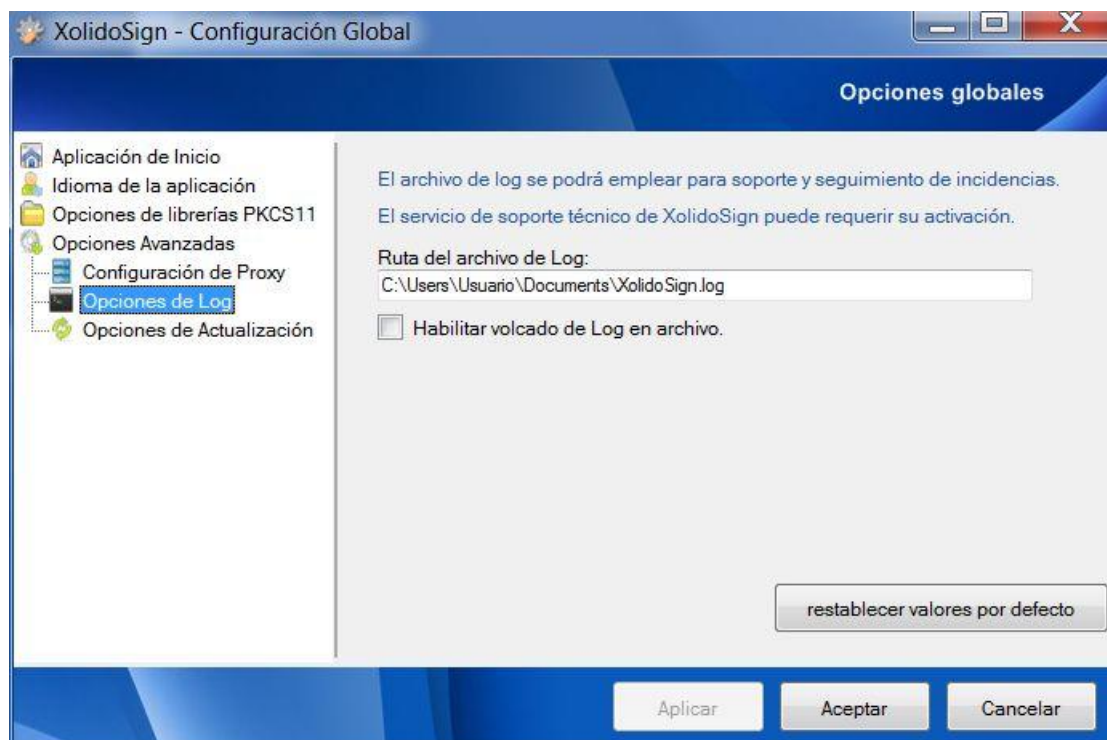


Fig. 6. Configuración del archivo de Log.

- Configuración de las opciones de Actualización

En esta pestaña se pueden habilitar o deshabilitar los **avisos de actualización** que aparecen al inicio de la aplicación. Por defecto esta opción aparece habilitada, de modo que se informa al usuario de forma automática en caso de que exista una nueva versión de Xolido®Sign. Es más que aconsejable permanecer actualizado por su seguridad ante cualquier nuevo algoritmo criptográfico implementado o mejora en la información avanzada incluida en las firmas electrónicas.

Se presenta también un botón, con el nombre **Comprobar actualización** que permite al usuario realizar la búsqueda inmediata de nuevas versiones de Xolido®Sign.

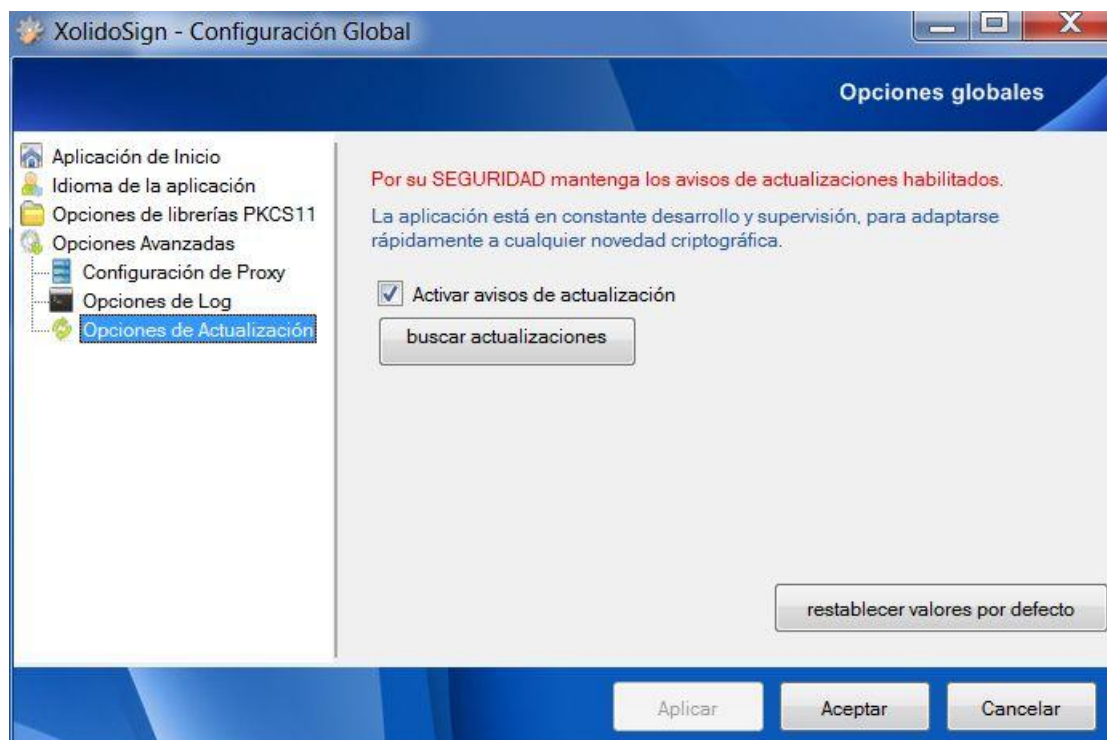


Fig. 7. Configuración de las opciones de actualización.

A continuación se presentan cada uno de las funcionalidades de la aplicación, incluyendo su forma de uso y si corresponde, las opciones propias de configuración.

3. Uso de la aplicación Xolido®Sign - Firmar



Fig. 8. Cómo usar la aplicación gratuita Xolido®Sign para firmar.

Xolido®Sign permite realizar la firma electrónica avanzada de los documentos que desee, garantizando así que el documento con el que se ha operado cumple la propiedad de integridad, no ha sido modificado desde su firma, y asegurando la identidad del autor o firmante.

Una vez realizado el proceso de firma electrónica, dispondrá de los archivos firmados en la carpeta seleccionada, acompañados de los archivos de firma digital.

Si trabaja con documentos Adobe PDF, podrá elegir la opción de incrustar la firma electrónica en el propio archivo, en cuyo caso no se creará archivo de firma digital independiente.

A continuación se muestra una imagen con la interfaz correspondiente a la ventana principal de Xolido®Sign - Firmar.

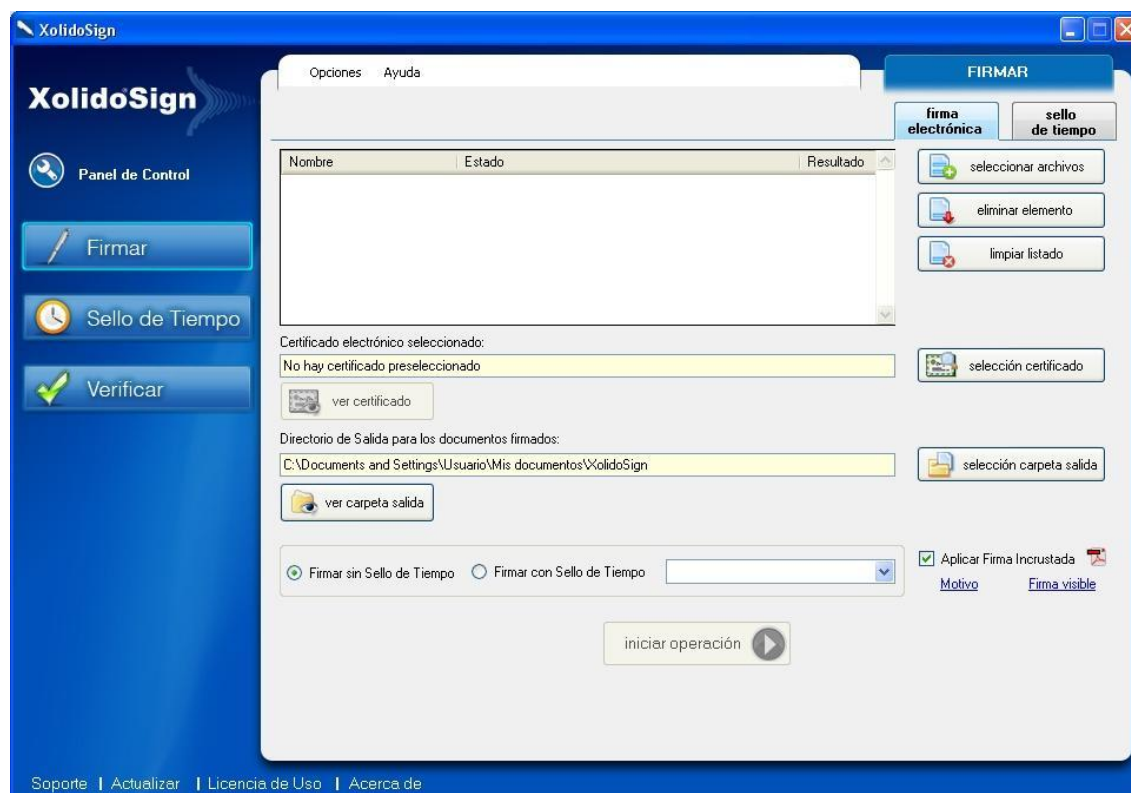


Fig. 9. Interfaz de la pantalla principal de Xolido® Sign para Firmar.

Se pueden apreciar diferentes zonas dentro de la interfaz de la aplicación, cada una de las cuales se ocupa de completar pequeñas operaciones que guiarán al usuario hacia el objetivo final, que es la firma digital con o sin sello de tiempo de documentos a los que tenga acceso.

3.1. Zona de Gestión de Documentos

En la interfaz gráfica se presenta, en primer lugar, un bloque de tres opciones relacionadas con la gestión de archivos accesibles por el usuario, bien en su propio ordenador o en una red local.

La primera opción (**Seleccionar Archivos**) conduce al usuario a un cuadro de diálogo de Windows para que complete la selección de todos los archivos que desea incluir en el procedimiento de firma digital o sellado de tiempo.

La selección puede ser múltiple de modo que la aplicación reporta un importante ahorro de tiempo para el usuario que necesita firmar un gran número de documentos. Para realizar dicha selección múltiple mantenga pulsada la tecla *Ctrl* de su teclado a la vez que va seleccionando los diferentes archivos deseados, para a continuación aceptar la selección en el cuadro de diálogo.

Una vez seleccionado los archivos que se desean firmar o sellar, el sistema le mostrará una tabla con los datos relativos al **Nombre**, **Estado** y **Resultado** de cada uno de ellos.

Las propiedades de Estado y Resultado hacen referencia a la situación en cada momento de espera, éxito en la operación... en la que se encuentra cada uno de los documentos seleccionados.

La segunda opción, (**eliminar elemento**), le permitirá suprimir del listado de documentos seleccionados aquellos que no desee firmar o sellar, y la tercera opción (**limpiar listado**) permite suprimir de forma rápida todos los documentos de la selección.

A continuación se muestra una imagen con un caso práctico de esta Zona de Gestión de Documentos en el transcurso de una operación de Firma o Sello de Tiempo.

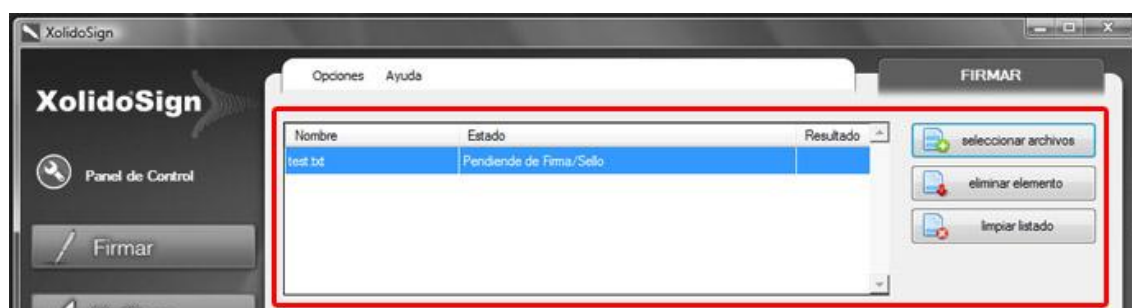


Fig. 10. Zona de Gestión de Documentos con información durante la operación.

3.2. Zona de Gestión de Certificados Electrónicos

Para realizar la operación de firma digital es necesario estar en posesión de un certificado electrónico, y por lo tanto la aplicación se ha de ocupar de la correcta selección del mismo dentro de un “repositorio de certificados”, que en este caso, para facilitar la labor al usuario, se trata del propio Almacén de Certificados de Windows.

También están soportados los certificados alojados de forma externa en lo que se conoce como tarjetas criptográficas. Un ejemplo empleado muy frecuentemente en la actualidad es el DNI electrónico, **DNle**, que con solo conectarlo al dispositivo de lectura de tarjetas será detectado por Windows e incluido en su almacén de certificados, por lo que podrá ser usado con total comodidad en Xolido® Sign.

La interfaz de la aplicación presenta la opción **Selección Certificado** para presentar un listado de certificados electrónicos disponibles y que el usuario pueda escoger el que desee en cada momento para realizar la firma digital de los documentos seleccionados.

La aplicación realiza las comprobaciones necesarias para determinar los parámetros de validación del certificado, fecha de inicio y fin de su periodo de validez, correcta estructura del certificado, consulta del estado de revocación...

Si la aplicación considera que el certificado elegido no es de total confianza, mostrará un aviso, permitiendo en cualquier caso al usuario continuar con el proceso de firma si así lo desea.

Además la interfaz mostrará los datos del certificado seleccionado, para poder visualizar de forma cómoda el certificado con el que está trabajando.

Si el usuario desea analizar al detalle el certificado electrónico escogido puede hacer *click* sobre la opción **Ver Certificado**, y se mostrará una ventana con todos los datos del mismo.

A continuación se muestra una imagen con la franja correspondiente a la citada selección de certificados.



Fig. 11. Zona de Gestión de Certificados Electrónicos.

3.3. Zona de Gestión de la Carpeta de Salida

El siguiente bloque de opciones permite al usuario establecer la carpeta en la que se guardarán los documentos y firmas o sellos de tiempo adjuntos.

La aplicación viene configurada por defecto para establecer como ruta una carpeta llamada Xolido® Sign dentro del directorio correspondiente a los Documentos del Usuario, sin embargo, se permite cambiar esta selección, para ello deberá pulsar en **Selección Carpeta Salida** y proceder a indicar la carpeta deseada para salvar los resultados de la operación de firma y/o sellado de tiempo.

La opción **Ver Carpeta Salida** mostrará el contenido de dicha carpeta a través de un explorador de Windows.

A continuación se muestra el fragmento de la interfaz que se corresponde con la zona de gestión de la carpeta de salida.



Fig. 12. Zona de Gestión de la Carpeta de Salida.

3.4. Zona de Gestión de las Opciones de Operación

En esta sección de la interfaz se debe configurar la opción de operación que se desea realizar para los archivos seleccionados.

Tenemos diferentes posibilidades, que se detallan a continuación:

- **Firmar sin Sello de Tiempo**

La operación que se realizará es la firma digital sin incrustar una marca de hora para el momento en que dicha firma se lleva a cabo.

- **Firmar con Sello de Tiempo**

Seleccionando esta opción la firma digital llevará incrustada una marca con la fecha y hora correspondiente al momento en que se ha realizado la operación de firma.

Sirve para dar validez a la firma digital a partir de un instante de tiempo determinado y validado por su sello temporal.

Esta opción presenta a la derecha en la interfaz gráfica una lista desplegable con los servidores de sello de tiempo configurados en Xolido® Sign para permitir al usuario cambiar en el acto para la operación que va a realizar el servidor utilizado para añadir la marca de tiempo fiable a la firma digital.

- **Aplicar Firma Incrustada en PDF**

Cuando seleccionamos una de las opciones para firmar digitalmente los documentos tenemos a nuestra disposición la posibilidad de operar de forma diferente con los documentos Adobe PDF.

En este tipo de archivos la firma digital puede ir incrustada en el propio documento, de forma que no se incluirá en la carpeta de salida el documento a firmar y su firma asociada por separado tal y como ocurre con el resto de tipos de archivo, sino que se incluye solamente un documento PDF, con el mismo nombre que el documento original a firmar pero con la firma digital ya incrustada debidamente.

De esta forma, cualquier tercero que disponga del visor de PDF gratuito de Adobe (**Adobe Reader**), puede recibir y verificar correctamente los PDF firmados y analizar tanto la identidad del firmante como el instante en que se ha producido la firma y la entidad servidora de tiempo que avala dicho instante temporal (en caso de haber marcado la opción de *Firma con Sello de Tiempo*).

Una de las múltiples ventajas de Xolido® Sign radica en la posibilidad de realizar la firma incrustada en múltiples documentos PDF de forma totalmente desatendida, con un solo *click* y total agilidad, todo ello de forma absolutamente gratuita.

Además, la aplicación presenta un acceso directo a la configuración de las firmas integradas en PDF, en especial para los campos de motivo y localización, así como también un acceso directo a la configuración de la firma visible en PDF.

A continuación se muestra una imagen con la zona de la interfaz relacionada con la selección de opciones de operación que se acaba de explicar.

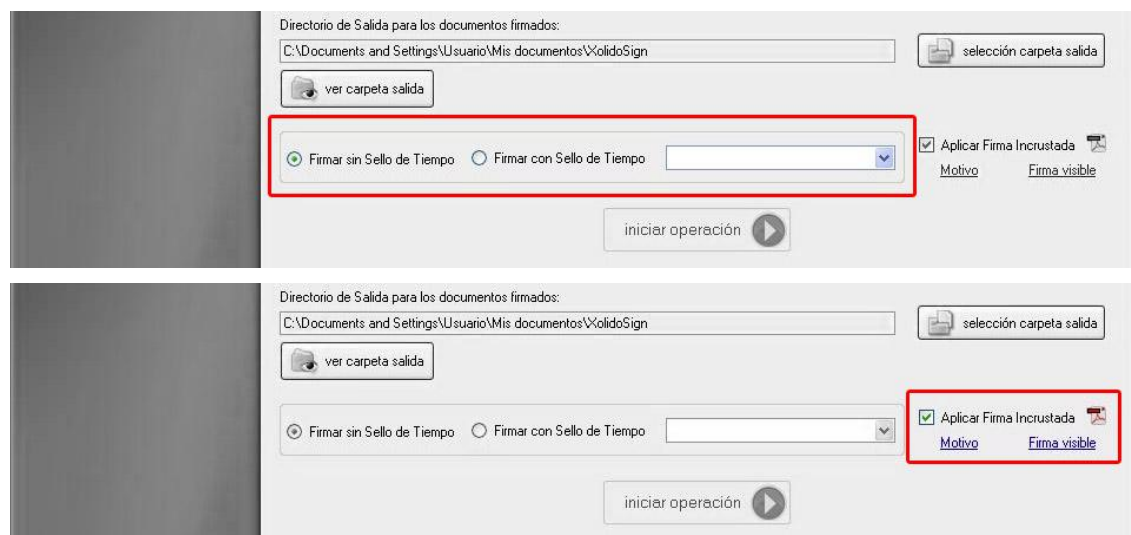


Fig. 13. Zona de Gestión de las Opciones de Operación.

3.5. Zona de Inicio de Operación

Una vez realizadas todas las operaciones descritas anteriormente, podrá realizar la firma digital de todos los documentos seleccionados, simplemente haciendo click en el botón **iniciar operación**, de forma rápida y automática.

Este botón de inicio no estará disponible hasta que no se hayan completado correctamente la selección de al menos un archivo y un certificado para firmar.

A continuación se muestra una imagen con esta última sección de la interfaz de la aplicación.



Fig. 14. Zona de Inicio de la Operación.

4. Uso de la aplicación Xolido®Sign – Sello de tiempo



Fig. 15. Cómo usar la aplicación gratuita Xolido®Sign para Sello de Tiempo.

Xolido®Sign permite aplicar sellos de tiempo a todos tus documentos y archivos, de forma que se garantiza la existencia de los mismos en un instante de tiempo determinado, y se asegura que el archivo o documento cumple la propiedad de integridad, no ha sido modificado desde su sellado temporal.

Una vez realizado el proceso de sello de tiempo independiente, dispondrá de los archivos sellados en la carpeta seleccionada, acompañados de los archivos de sello de tiempo digital.

A continuación se muestra una imagen con la interfaz correspondiente a la ventana principal de Xolido®Sign – Sello de Tiempo.

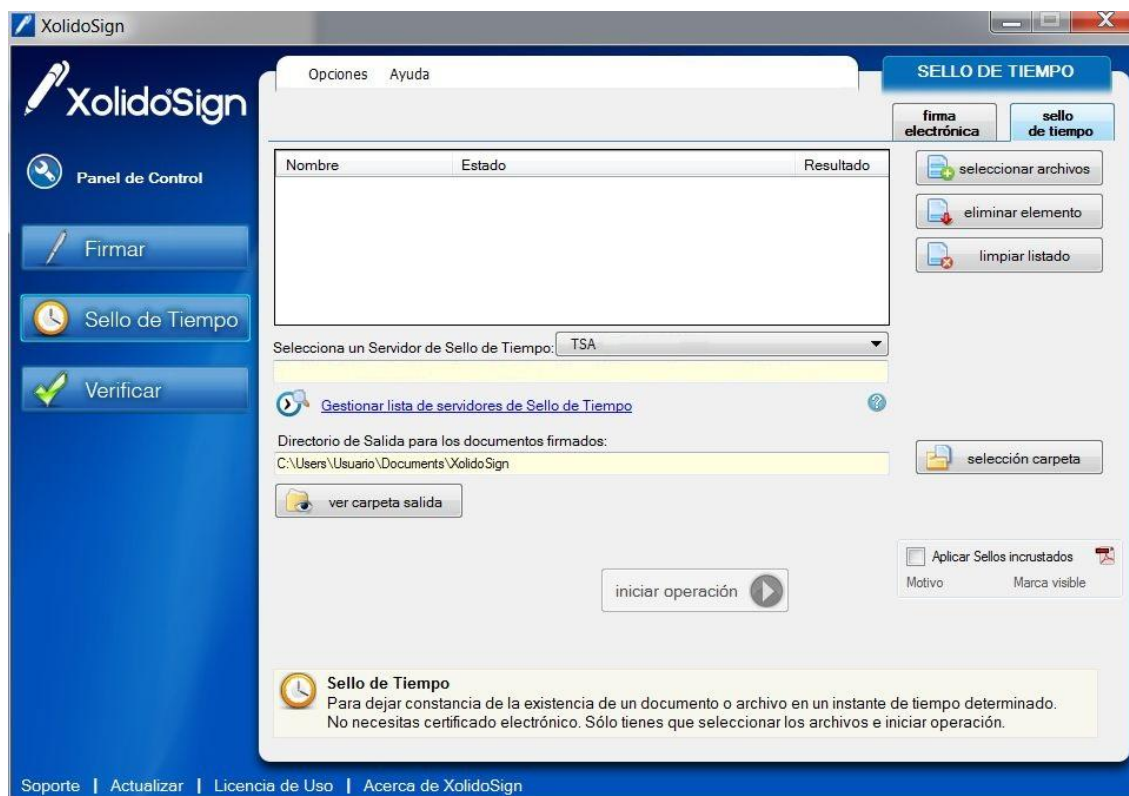


Fig. 16. Interfaz de la pantalla principal de Xolido® Sign para Sello de Tiempo.

4.1. Zona de Gestión de Documentos

En la interfaz gráfica se presenta, en primer lugar, un bloque de tres opciones relacionadas con la gestión de archivos accesibles por el usuario, bien en su propio ordenador o en una red local.

La primera opción (**Seleccionar Archivos**) conduce al usuario a un cuadro de diálogo de Windows para que complete la selección de todos los archivos que desea incluir en el procedimiento de firma digital o sellado de tiempo.

La selección puede ser múltiple de modo que la aplicación reporta un importante ahorro de tiempo para el usuario que necesita firmar un gran número de documentos. Para realizar dicha selección múltiple mantenga pulsada la tecla *Ctrl* de su teclado a la vez que va seleccionando los diferentes archivos deseados, para a continuación aceptar la selección en el cuadro de diálogo.

Una vez seleccionado los archivos que se desean firmar o sellar, el sistema le mostrará una tabla con los datos relativos al **Nombre**, **Estado** y **Resultado** de cada uno de ellos.

Las propiedades de Estado y Resultado hacen referencia a la situación en cada momento de espera, éxito en la operación... en la que se encuentra cada uno de los documentos seleccionados.

La segunda opción, (**eliminar elemento**), le permitirá suprimir del listado de documentos seleccionados aquellos que no desee firmar o sellar, y la tercera opción (**limpiar listado**) permite suprimir de forma rápida todos los documentos de la selección.

Esta zona es similar a la existente para la funcionalidad de Firma de Xolido® Sign.

4.2. Zona de Gestión de Servidor de Sello de Tiempo

La siguiente zona de la interfaz presenta una lista desplegable con los nombres identificativos de las distintas autoridades de sellado de tiempo (TSA) que se han configurado en Xolido® Sign.

El usuario puede escoger el servidor de sello de tiempo de la autoridad TSA con la que desee realizar el sellado de tiempo de los documentos seleccionados en el paso anterior.

Además se presenta en un cuadro de texto una breve descripción de la autoridad TSA escogida, e incluso indicando la dirección URL del servidor en los casos que procede.

También aparece un enlace para acceder a **gestionar servidores**, mediante el que se establece un acceso directo a las opciones del configurador relacionadas con las autoridades de sellado de tiempo (TSA) dadas de alta en Xolido® Sign y que luego aparecerán en los listados desplegables como opciones a elegir por el usuario.

A continuación se muestra una imagen con la región de interfaz gráfica correspondiente a la gestión y selección del servidor de sello de tiempo.

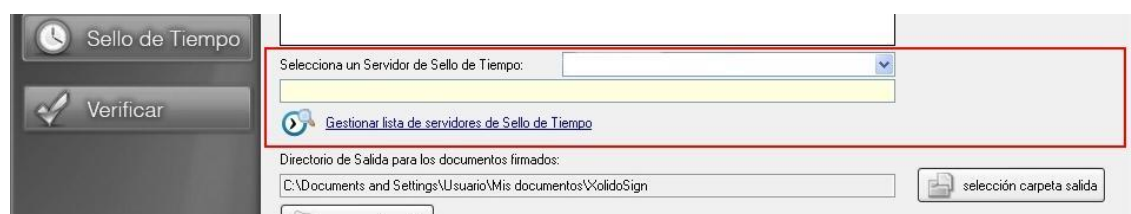


Fig. 17. Zona de Gestión del Servidor de Sello de Tiempo.

4.3. Zona de Gestión de la Carpeta de Salida

El siguiente bloque de opciones permite al usuario establecer la carpeta en la que se guardarán los documentos y firmas o sellos de tiempo adjuntos.

La aplicación viene configurada por defecto para establecer como ruta una carpeta llamada Xolido®Sign dentro del directorio correspondiente a los Documentos del Usuario, sin embargo, se permite cambiar esta selección, para ello deberá pulsar en **Selección Carpeta Salida** y proceder a indicar la carpeta deseada para salvar los resultados de la operación de firma y/o sellado de tiempo.

La opción **Ver Carpeta Salida** mostrará el contenido de dicha carpeta a través de un explorador de Windows.

La interfaz correspondiente es análoga a la mostrada para la misma zona de gestión en la funcionalidad de Xolido®Sign para Firmar.

4.4. Zona de Opciones de Operación

El siguiente bloque muestra la opción de operación que se incorpora para permitir el proceso específico de los sellos de tiempo independientes en el caso de manejar documentos de tipo PDF.

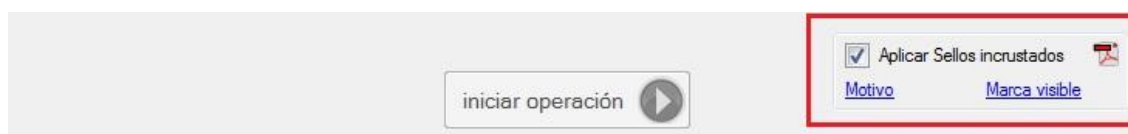


Fig. 18. Zona de Opciones de Operación.

- Aplicar Sellos de tiempo incrustados en PDF

Con Xolido®Sign es posible escoger la opción de incrustar el sello de tiempo en la propia estructura de los documentos PDF.

De esta forma, en la carpeta de salida no aparecerá el documento PDF y su sello de tiempo asociado por separado tal y como ocurre con el resto de tipos de archivo, sino que se incluiría solamente un documento PDF, con el mismo nombre que el documento original a sellar con tiempo pero con el sello de tiempo digital ya incrustado debidamente.

De esta forma, cualquier tercero que disponga del visor de PDF gratuito de Adobe (**Adobe Reader a partir de la versión 10**), puede recibir y verificar correctamente los PDF sellados con tiempo y analizar el instante en que se ha producido el sello del documento y la entidad servidora de tiempo que avala dicho instante temporal.

4.5. Zona de Inicio de Operación

Una vez realizadas todas las operaciones descritas anteriormente, podrá realizar el sellado de tiempo de todos los documentos seleccionados, simplemente haciendo click en el botón **iniciar operación**, de forma rápida y automática.

Este botón de inicio no estará disponible hasta que no se hayan completado correctamente la selección de al menos un archivo y se disponga de por lo menos un proveedor de servicios de sellado de tiempo TSA, es decir, Xolido®Sign tiene al menos configurado un servidor de sello de tiempo disponible para su uso.

A continuación se muestra una imagen con esta última sección de la interfaz de la aplicación.

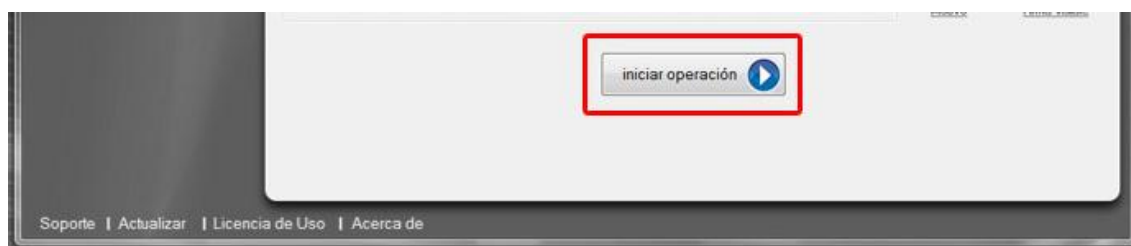


Fig. 19. Zona de Inicio de la Operación.

5. Guía de Configuración de Xolido® Sign – Firmar y Sello de Tiempo

En esta sección se van a presentar las diferentes opciones de configuración soportadas por la aplicación para las funcionalidades de firma electrónica y sello de tiempo. Los cambios que se efectúan en dicha configuración son globales y compartidos por ambas funcionalidades.

Señalar que las opciones del menú de configuración están pensadas para agilizar aún más el funcionamiento y los pasos a seguir para completar la firma electrónica y el sellado de tiempo de documentos y archivos.

A continuación se muestra una imagen para poder visualizar gráficamente la forma de acceder al menú de configuración de Xolido® Sign. Además se puede acceder mediante la tecla *F5* de acceso rápido desde cualquiera de las funcionalidades (firma digital y sello de tiempo).

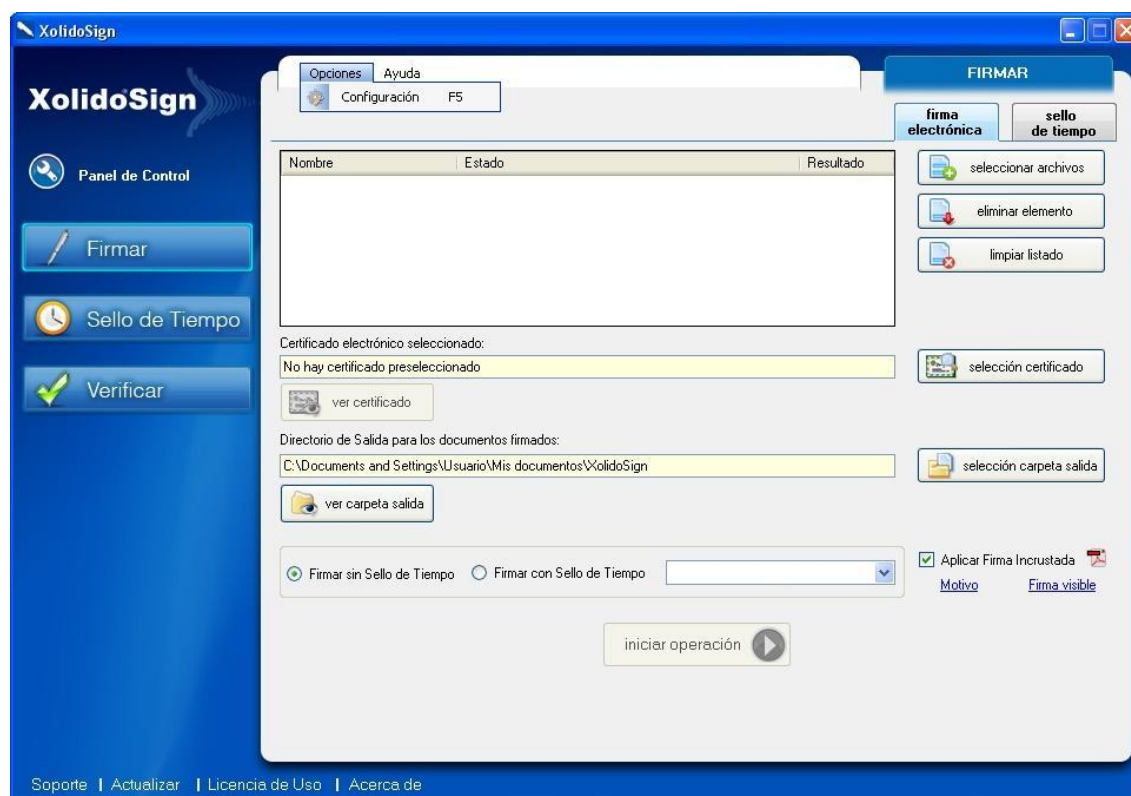


Fig. 20. Acceso al Menú de Configuración de Xolido® Sign.

El menú de configuración está dividido en diferentes pestañas, cada una de las cuales asociadas a un posible aspecto configurable dentro de la aplicación, de forma que resulte lo más intuitivo posible para el usuario.

5.1. Zona de Opciones de Certificados

El primer grupo de opciones de configuración se refiere a las opciones relacionadas con los certificados electrónicos.

5.1.1 – Selección de certificado

En primer lugar está la Selección de certificado, donde se puede configurar el Certificado Electrónico por defecto usado por Xolido®Sign. Al hacer *click* sobre el botón **Configurar Certificado por Defecto** se solicita al usuario la selección de uno de los certificados electrónicos disponibles.

Si la selección se completa correctamente, el certificado se presentará a partir de ahora al iniciar la aplicación como el certificado preseleccionado y no habrá que llevar a cabo el paso de selección si se desea trabajar con dicho certificado pre configurado, ahorrando de esta forma un paso del proceso a los usuarios de Xolido®Sign.

En el panel mostrado también se presenta una breve descripción del certificado preseleccionado, en caso de haberlo, y se puede analizar también el certificado en detalle, pulsando la opción **Ver Certificado Configurado**.

En todo caso, los cambios son reversibles, pudiendo volver a la configuración por defecto simplemente haciendo *click* sobre el botón **restablecer valores por defecto**.

La imagen a continuación muestra este primer bloque de opciones.

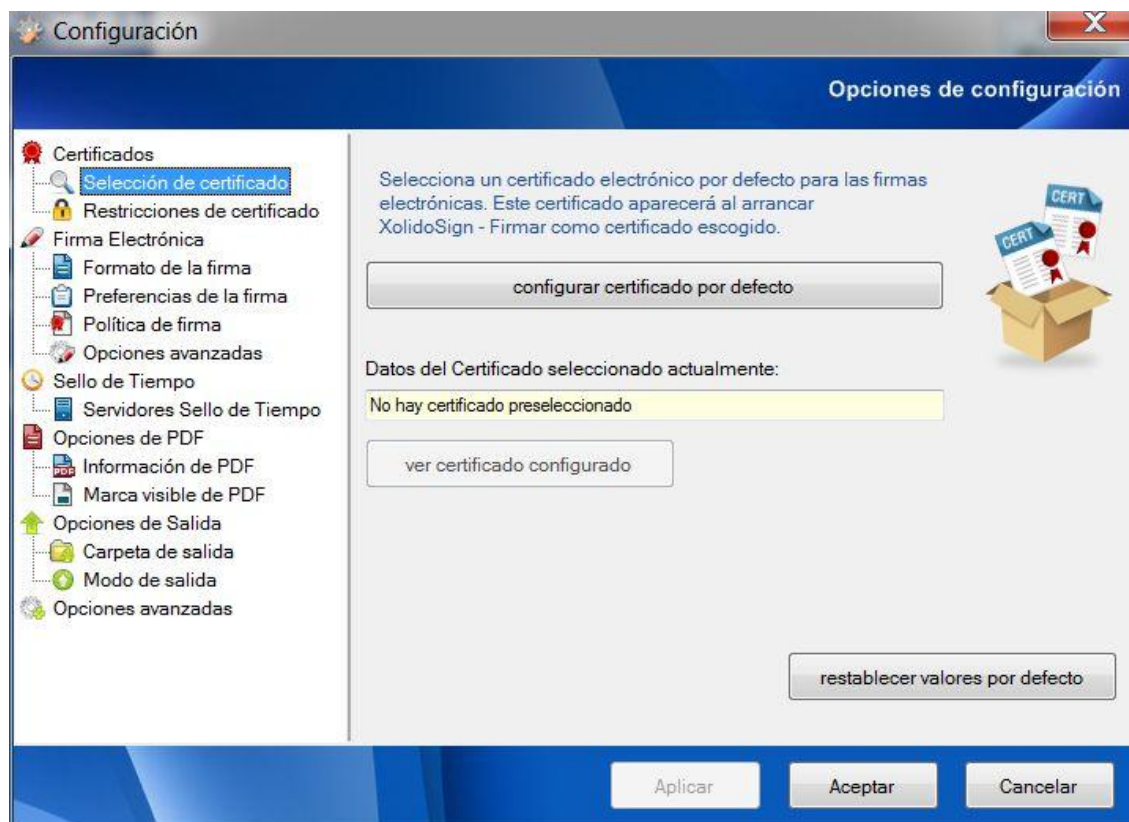


Fig. 21. Opciones de Certificados. Selección de certificado.

5.1.2 – Restricciones de certificado

En segundo lugar están las opciones relacionadas con las Restricciones a aplicar para los certificados durante la operativa de Xolido®Sign.

Se permite configurar restricciones de seguridad para el usuario, de modo que éste pueda indicar a Xolido®Sign la obligatoriedad en el uso de **certificados que no se encuentren revocados, certificados que no se encuentren caducados** y que contemplen de forma explícita la **firma digital de documentos entre sus propósitos**.

Por defecto, la aplicación realiza la comprobación online del estado de revocación de los certificados, conectándose a las autoridades certificadoras correspondientes. Un usuario puede desear omitir estas comprobaciones online, por ejemplo por estar en un ordenador que no dispone temporalmente de conexión a Internet.

Para ello deberá deseleccionar la opción correspondiente etiquetada como **Comprobar Online el Estado de Revocación de los Certificados**.

Mediante la opción **Consultar la validez del certificado electrónico al arrancar**, el usuario puede asegurarse de que la aplicación compruebe online la validez del Certificado Preseleccionado cada vez que se ejecute la aplicación.

Además, la aplicación realiza una nueva consulta a las entidades certificadoras para obtener los valores de revocación de los certificados, en el caso de disponer de mecanismos de revocación proporcionados por la autoridad de certificación correspondiente (CA), justo antes de comenzar el proceso de firma electrónica, almacenando internamente esta información y procediendo a actualizarla mediante una nueva petición una vez finalizado el tiempo de validez de la **caché de revocación** interna, cuya duración puede definir el usuario en el campo correspondiente, tal y como se observa en la imagen a continuación.

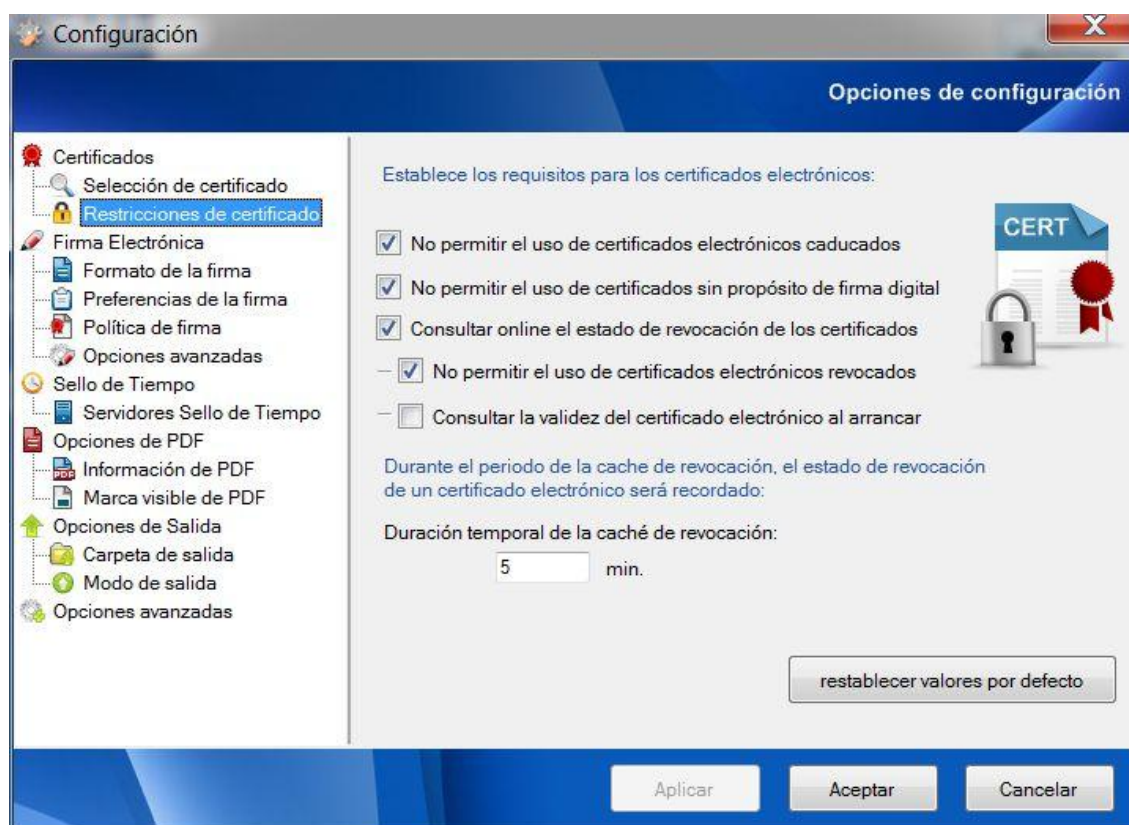


Fig. 22. Opciones de Certificados. Restricciones de certificado.

5.2. Zona de Opciones de Firma

Esta sección del panel de configuración es responsable de gestionar las opciones y ajustes que conlleven un cambio en el tipo de firma electrónica realizada por la aplicación.

5.2.1 – Formato de la firma

En el primer bloque de opciones se puede configurar el formato preferido para la firma electrónica.

Primero el usuario puede seleccionar una de los modos de operación disponibles:

- **Realizar firmas electrónicas básicas. (Perfil –BES; ej. CMS / CAdES-BES)**

Mediante esta opción el usuario realizará las firmas básicas válidas acorde al estándar correspondiente (Por ejemplo: RFC. 3852 - *Cryptographic Message Syntax* (CMS)) del organismo IETF.

- **Realizar firmas electrónicas con referencias de certificados y revocación. (Perfil –C; ej. CAdES-C)**

Con esta opción la aplicación añade en las firmas electrónicas las referencias a los certificados empleados en la firma electrónica y las referencias a los valores de revocación obtenidos o disponibles para dichos certificados empleados en el proceso de firma, ambos como atributos no firmados, siguiendo el estándar IETF (RFC. 5126 - *CMS Advanced Electronic Signatures*) y la recomendación ETSI para firmas electrónicas avanzadas (ETSI TS 101 733).

- **Realizar firmas electrónicas completas y extendidas incluyendo valores de certificados y revocación. (Perfil –XL; ej. CAdES-XL)**

Si la aplicación opera en este modo de funcionamiento, las firmas electrónicas, además de las referencias de los certificados y valores de revocación correspondientes que se añadían en la opción previa (Perfil -C), incluirán los valores propiamente de los certificados empleados en el proceso y los objetos de revocación correspondientes a cada uno de los certificados implicados en la firma electrónica, en caso de estar disponibles.

Si los valores de revocación no son accesibles, bien debido a que el certificado no tenga servicio de revocación, o éste no se encuentre accesible a terceros, se incluirá una estructura indicativa de la situación hallada para poder transmitir dicha información al receptor de la firma.

Se agregará esta información como atributo no firmado, cumpliendo las directivas recogidas en el estándar IETF (RFC. 5126 - *CMS Advanced Electronic Signatures*) y la recomendación ETSI para firmas electrónicas avanzadas (ETSI TS 101 733).

Para las firmas electrónicas incrustadas en PDF, la información de los correspondientes valores de certificados y revocación se añade de acuerdo a la referencia establecida por Adobe en su *PDF Reference 1.6* y superiores.

Con estas firmas electrónicas se alcanza la confiabilidad avanzada para los archivos de firma electrónica generados por la aplicación.

Se muestra a continuación la imagen de dicho grupo de opciones.

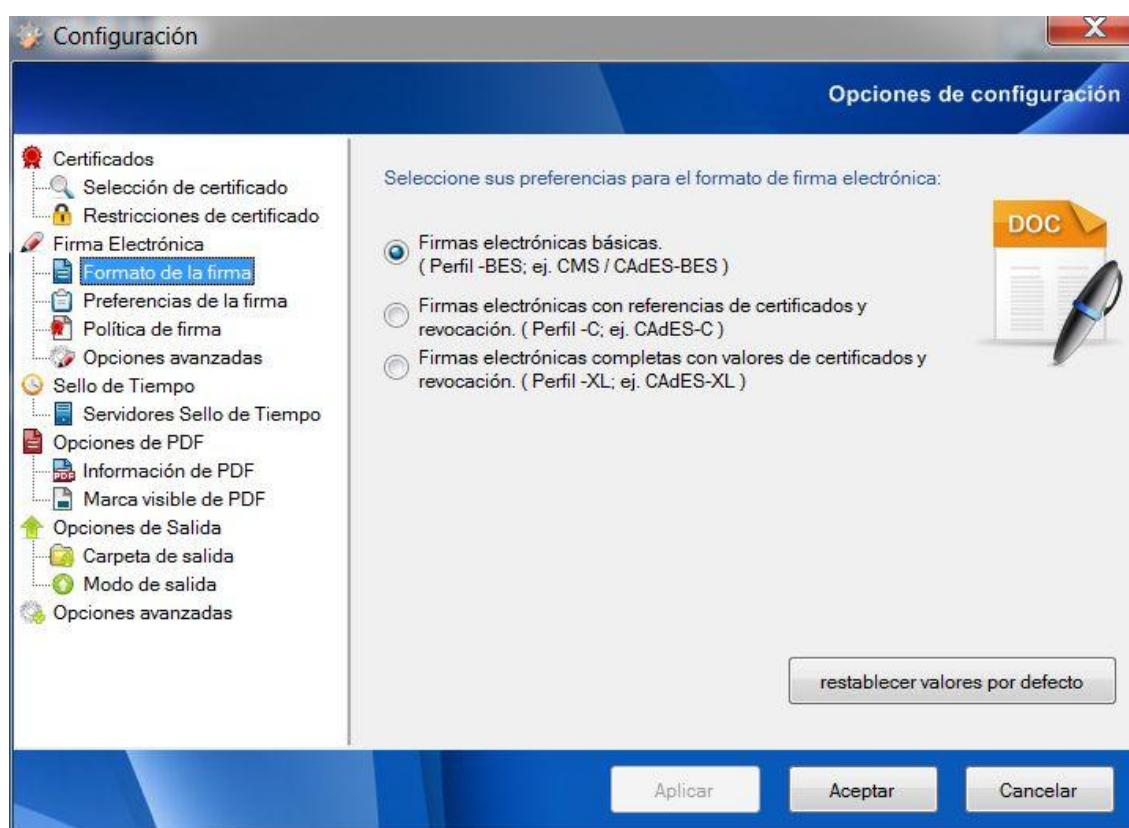


Fig. 23. Opciones de Firma Electrónica. Formato de la firma.

5.2.2 – Preferencias de la firma

El siguiente grupo de opciones sirve para establecer aspectos adicionales de preferencia para que Xolido® Sign lo aplique en sus procesos de firma electrónica.

Entre las opciones tenemos la posibilidad de indicarle la realización de **firma incrustada en PDF por defecto** (siguiendo el perfil de compatibilidad PAdES-CMS, con las especificaciones agregadas de Adobe en su documentación de referencia *Adobe PDF Reference* para las referencias y valores de revocación cuando éstos sean agregados a la firma electrónica). Mediante esta opción, Xolido® Sign detecta de forma automática los documentos PDF dentro del listado seleccionado para firmar y procede a realizar con ellos la firma incrustada en el propio documento. Esta opción selecciona por defecto *Aplicar Firma incrustada PDF* existente en la pantalla principal de la aplicación.

Incluso se ofrece la posibilidad de incrustar las **firmas electrónicas de forma acorde al perfil PAdES-BES**, que no se encuentra activado por defecto dado que sólo es compatible desde la versión de lectores PDF Adobe Reader 10 en adelante, hecho que se advierte en la propia pantalla de configuración.

A continuación se presenta la opción para **Seleccionar la Opción Firma con Sello de Tiempo por defecto**. Si se encuentra activa esta opción se preseleccionará dentro de la interfaz principal de Xolido® Sign la opción *Firma con Sello de Tiempo* y se realizan las conexiones oportunas con el servidor de sello de tiempo que se haya declarado y configurado en la aplicación para la obtención del sellado de tiempo a agregar en la firma electrónica.

También se deja la posibilidad de que los usuarios opten por cancelar las firmas digitales en caso de no estar disponible la conexión al servidor de sello de tiempo y haber escogido el modo de operación *Firma con Sello de Tiempo*. Esta opción se corresponde con la etiqueta **Cancelar la Firma si el sellado de tiempo no está disponible**.

El efecto que tiene esta opción es el de no proceder a completar la operación de firma digital con sellado de tiempo en caso de no haber podido obtener un sello de tiempo válido desde el Servidor de Tiempo configurado.

Cuando esta opción no está seleccionada y se realiza *Firma con Sello de Tiempo*, en caso de no disponibilidad del servicio de sello de tiempo, la operación finalizará notificando éxito pero la firma realizada no incluirá dicho sello de tiempo.

También se añade la opción de **Cancelar la Firma si el certificado dispone de mecanismos de acceso a la información de revocación pero falla al obtener los datos**. En esta situación, la aplicación anula la operación de firma electrónica avisando al usuario si no ha podido conseguir la información de revocación (CRL u OCSP) siempre y cuando el certificado empleado disponga de la información completa y necesaria para el acceso a dicha información de revocación. Esta opción no tendrá efecto para la situación en la que los certificados empleados no dispongan de un servicio de

revocación o bien se estén empleando firmas de tipo básico PKCS7 / CMS, para las cuales el estándar determina que no se incrustan los valores de revocación en la propia construcción de la estructura de firma electrónica.

Se incluye la posibilidad de marcar **Realizar sellos de tiempo incrustados en PDF por defecto**, que pre-establece la funcionalidad de sellado de tiempo independiente incrustado como estructura de PDF de forma nativa. Ésta funcionalidad sólo está soportada desde la versión de Adobe Reader 10 en adelante.

En todo caso, los cambios son reversibles, pudiendo volver a la configuración por defecto de estas *Opciones de Certificados* simplemente haciendo *click* sobre el botón **restablecer valores por defecto**.

La imagen a continuación muestra los campos configurables explicados.

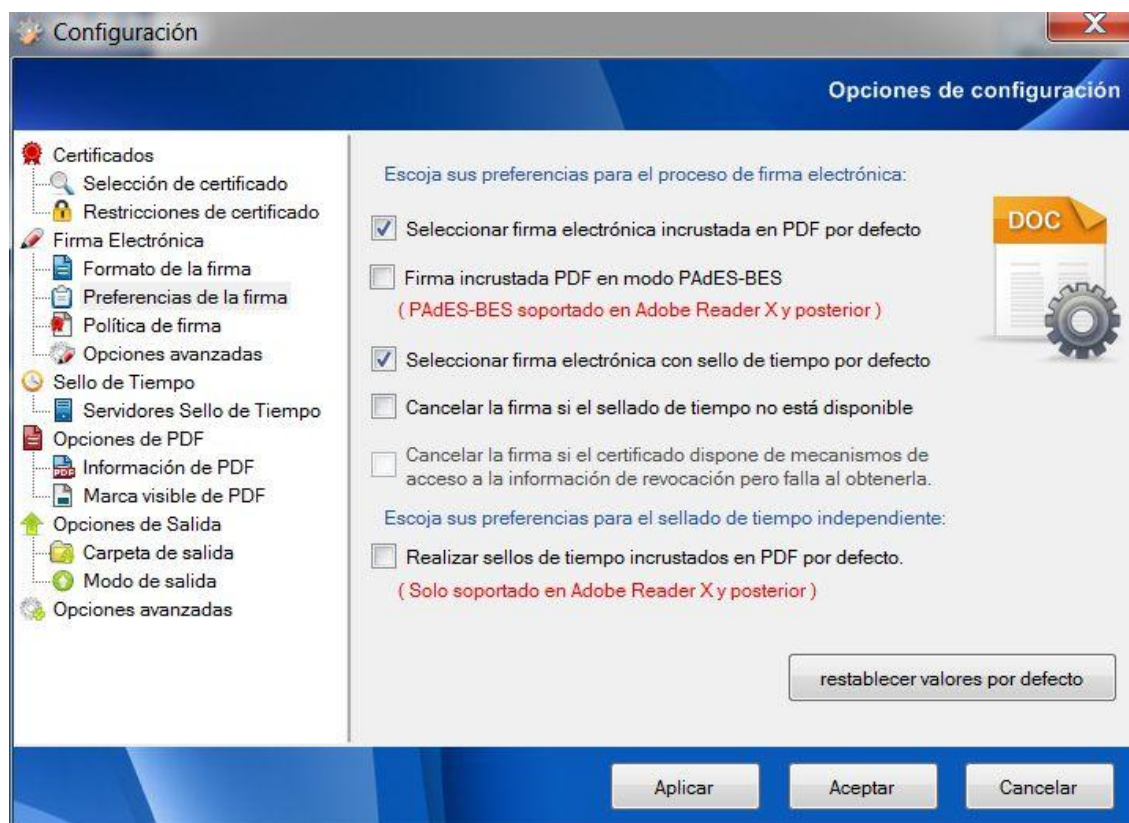


Fig. 24. Opciones de Firma Electrónica. Preferencias de la firma.

5.2.3 – Política de firma

Este bloque de opciones permite establecer los valores deseados en lo que respecta al compromiso del firmante y/o a la política de firma definida.

En primer lugar, se presentan las opciones para la selección del compromiso del firmante para las firmas electrónicas.

Mediante su uso, el firmante indica explícitamente al verificador, que, mediante la firma de los datos, ilustra un tipo de compromiso en nombre de sí mismo como firmante.

Los diferentes compromisos entre los que el firmante puede seleccionar el que desea aplicar en su proceso de firma electrónica son:

- *Origen*

El firmante reconoce haber creado, aprobado y enviado el mensaje.

- *Recepción*

El firmante reconoce haber recibido el contenido del mensaje.

- *Entrega*

El TSP proveedor de esta indicación ha despachado el mensaje en un almacén accesible al destinatario del mensaje.

- *Remitente*

La entidad que provee esta indicación ha enviado el mensaje (pero no necesariamente creado).

- *Aprobación*

El firmante ha aprobado el contenido del mensaje.

- *Creación*

El firmante ha creado el mensaje (pero no necesariamente aprobado o enviado).

Para agregar el compromiso a las firmas electrónicas realizadas, se deberá chequear la opción ***Insertar el compromiso del firmante en la firma.***

En el siguiente grupo de valores, se presentan los campos que permiten la definición de valores específicos para indicar una política de firma electrónica seguida por el firmante.

Los valores que componen esta información son: un identificador de la política (en formato OID), una URI que indicará la ubicación donde se encuentran los datos que componen la política, el algoritmo de resumen (hash) utilizado y el valor de resumen (hash) de dichos datos determinado mediante una cadena en formato Base64.

Para agregar la información de la política de firma, se deberá marcar la casilla ***Insertar valores de política en la firma.***

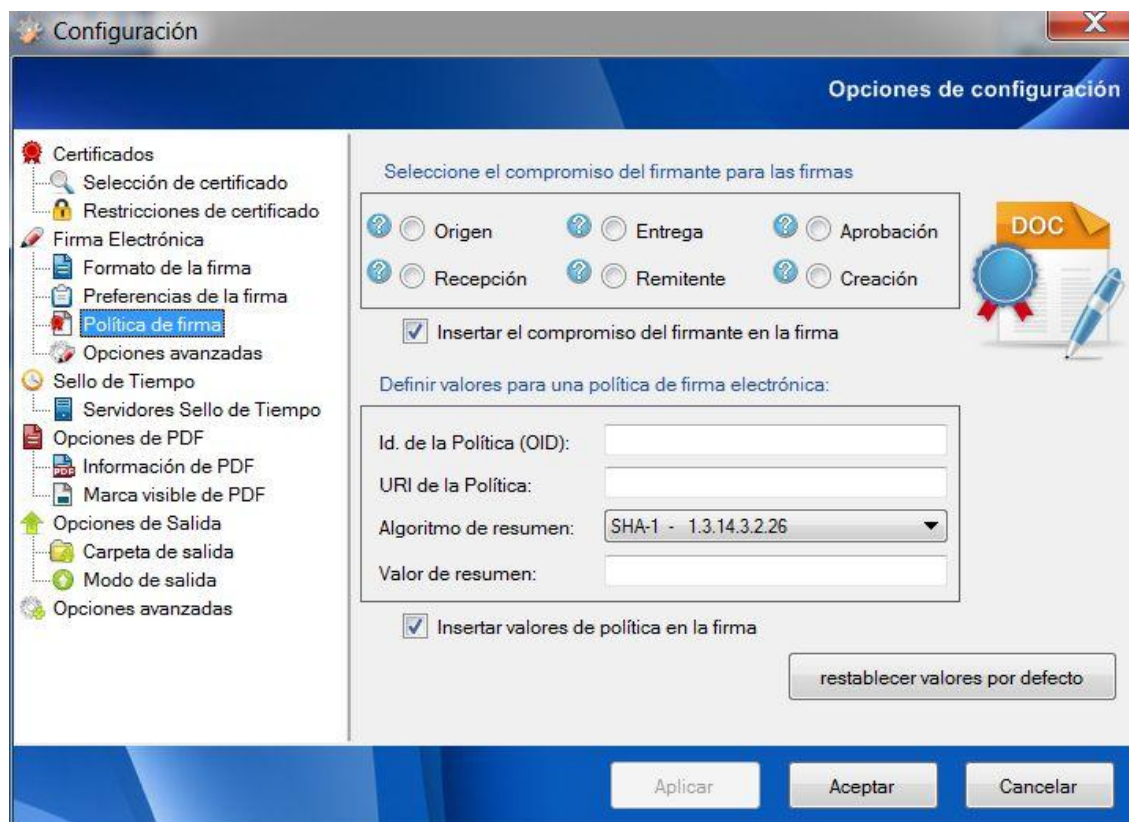


Fig. 25. Opciones de Firma Electrónica. Política de firma.

5.2.4 – Opciones avanzadas de firma electrónica

El siguiente grupo de configuraciones se refiere a Opciones Avanzadas para el proceso de firma, contemplando aspectos como el algoritmo de hash a utilizar por defecto (siendo SHA1 en la actualidad).

Además, se ofrecen dos opciones de parametrización de las firmas incrustadas en documentos PDF, que podrá emplear el usuario para lograr la compatibilidad con algunas aplicaciones de lectura de PDF con tratamiento especial de las firmas electrónicas incrustadas.

A continuación se muestra la imagen con dicho panel de opciones.

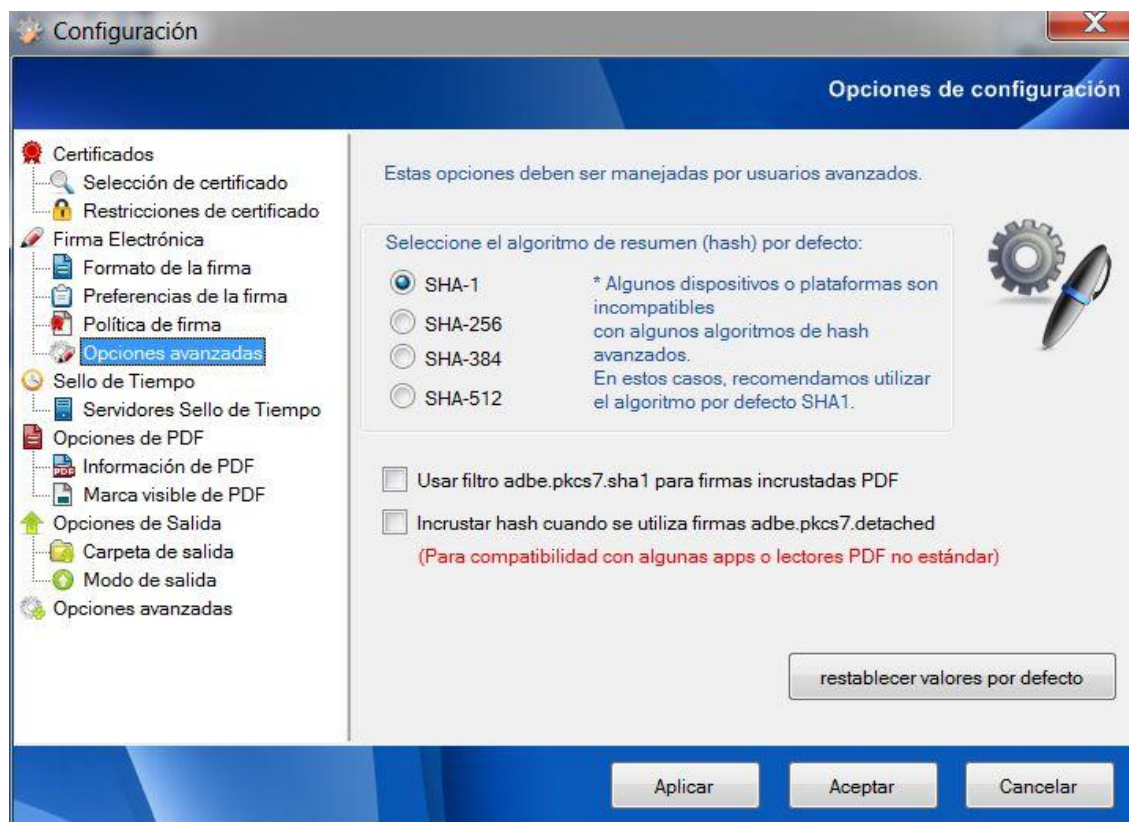


Fig. 26. Opciones de Firma Electrónica. Opciones avanzadas.

5.3. Zona de Sello de Tiempo

El siguiente grupo de configuraciones se refieren al servicio de Sello de Tiempo empleado por la aplicación para obtener tanto los Sellos de Tiempo independientes asociados a un determinado documento, como para los Sellos de Tiempo que se incrustan en los propios archivos de firma electrónica cuando se ha seleccionado esta posibilidad a la hora de iniciar la operación.

5.3.1 – Servidores de Sello de Tiempo

El Sello de Tiempo digital es un proceso de securización de la fecha de existencia de un documento o de una firma electrónica. La seguridad aquí hace referencia al hecho de que nadie, ni tan siquiera al propio creador o propietario del documento o firma le está permitido modificarlo, siempre y cuando la integridad de la entidad de sellado temporal no se encuentre en entredicho.

La imagen a continuación muestra la pestaña correspondiente a la gestión de los **servidores de sello de tiempo**.

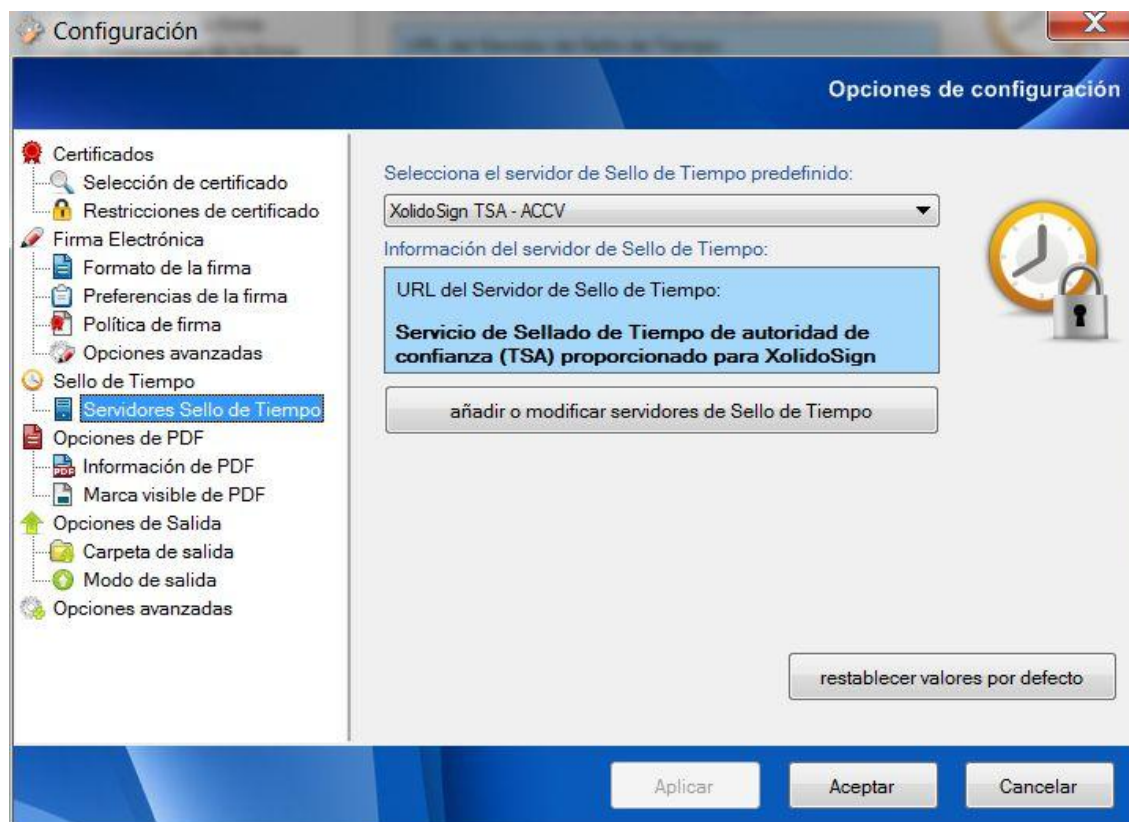


Fig. 27. Sello de Tiempo. Servidores de sellado de tiempo.

Accediendo a la opción *Añadir o Modificar Servidores de Sello de Tiempo*, se puede **gestionar la lista con varios servidores de sellado de tiempo (TSA)**, disponibles para la aplicación.

Para cada uno de los elementos el usuario de la aplicación puede establecer la **ruta de acceso al servidor** de tiempo, así como su nombre de **usuario** y **contraseña** en caso de que el servidor al que se pretende acceder para las peticiones de sellos temporales requiera autenticación. Además para cada servicio de sellado de tiempo que añada el usuario o venga establecido, se dispondrá de un **nombre identificativo**, para poder acceder a él de manera intuitiva a través de las listas desplegables.

A continuación se muestra una imagen del formulario de introducción de datos del servidor de sello de tiempo.



Fig. 28. Introducción de datos para un Servidor de Sello de Tiempo.

Los usuarios de Xolido®Sign pueden configurar el servidor de sellado de tiempo que consideren oportuno, siempre y cuando la dirección URL sea una dirección válida proporcionada por una entidad que realice Sellos de Tiempo digitales, seleccionando el deseado entre los disponibles mediante la lista desplegable presentada en la pestaña mostrada en la imagen.

En caso de seleccionar la opción **restablecer valores por defecto**, se volverán a mostrar las opciones de Servidores de Sellado de Tiempo incluidas en la aplicación Xolido®Sign, eliminándose aquellos servidores que provengan de la configuración específica del usuario.

5.4. Zona de Opciones de PDF

El siguiente grupo de opciones corresponde a las firmas electrónicas incrustadas en los documentos Adobe PDF.

5.4.1 – Información de firma PDF

En primer lugar encontramos la configuración de la Información de Firma PDF, donde se pueden editar dos campos de texto cuyo contenido aparecerá en la información referente a las firmas incrustadas en el propio documento PDF.

Se trata de los campos **Motivo de la firmas** y **Ubicación de las firmas**, el primero se emplea para indicar la razón por la que se procede a firmar el documento (aprobación del mismo, revisión, cierre del documento...) y el segundo hace referencia a la ubicación geográfica que se desea declarar para las firmas incrustadas.

En cualquier caso son valores informativos y su contenido es libre.

Además se puede indicar en este panel un valor de contraseña, para que el programa abra automáticamente los archivos PDF protegidos antes de proceder a completar una firma PDF incrustada. Se corresponde con la opción **Contraseña por defecto para la apertura de PDF protegidos**.

Si la contraseña de un archivo protegido PDF fuese distinta de lo pre configurado en este campo, se pedirá de forma interactiva al usuario durante el proceso de firma.

A continuación se presenta la imagen de dicho panel de configuración.

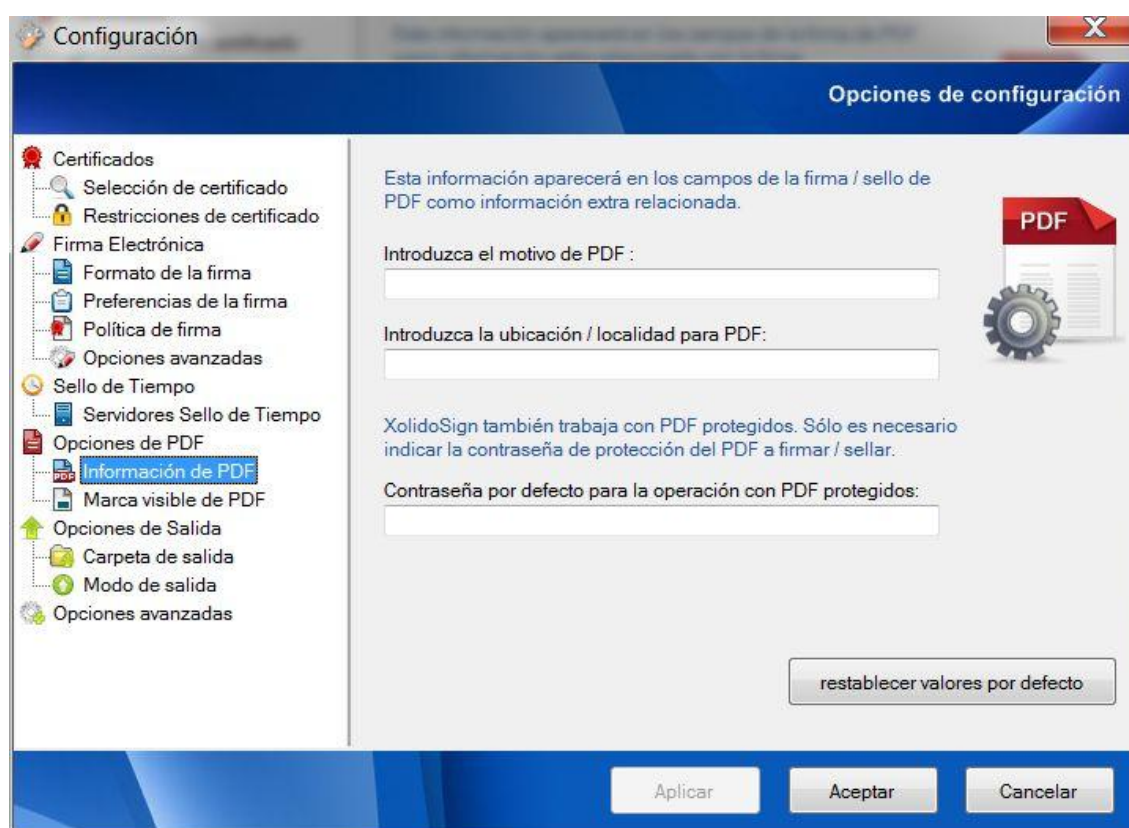


Fig. 29. Configuración de la Información de firma incrustada en PDF.

5.4.2 – Marca visible de la firma PDF

El siguiente grupo de configuraciones hacen referencia a la Marca visible de la firma PDF, que son las opciones disponibles a la hora de localizar una firma incrustada PDF de forma visible dentro del propio documento.

A continuación se incluye la imagen con este grupo de configuraciones:

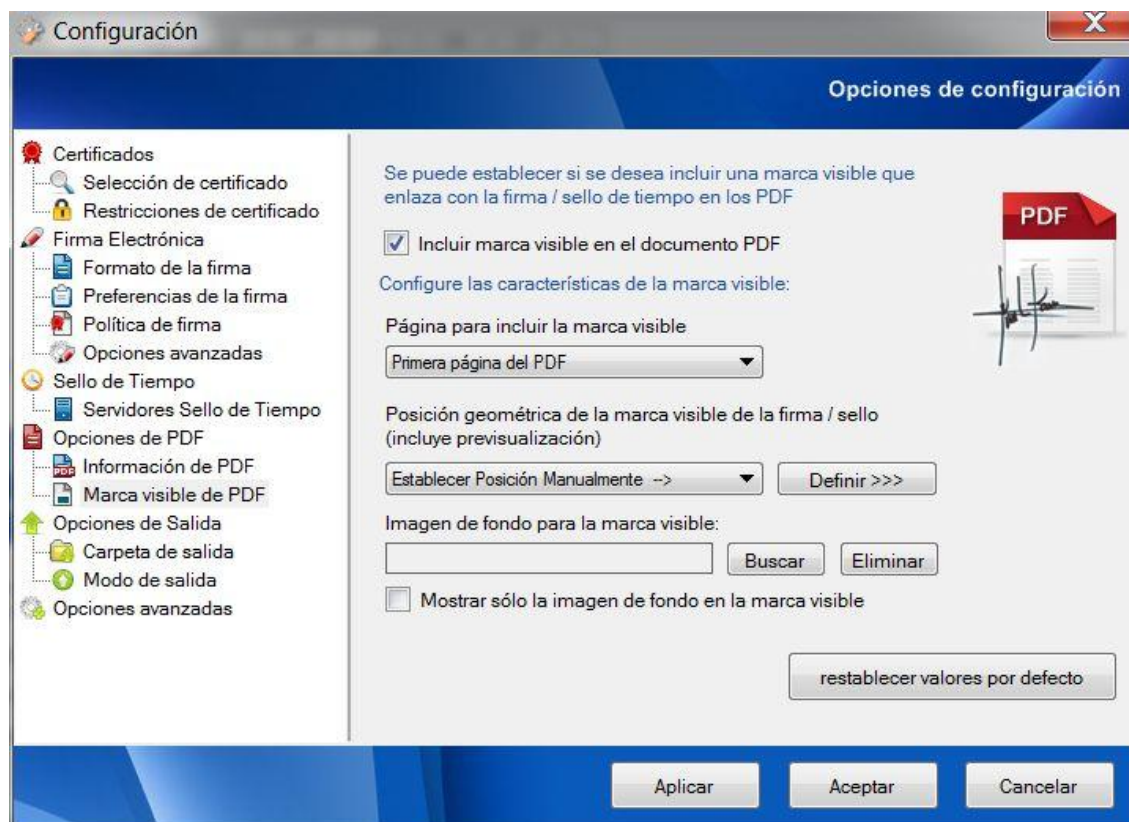


Fig. 30. Configuración de la marca visible de la firma incrustada en PDF.

En este panel lo primero que se puede marcar la opción **Incluir marca visible de la firma electrónica PDF**, mediante la cual se agregará de forma gráfica el enlace a la firma electrónica incrustada en el documento PDF.

Esta funcionalidad de marca visible de firma de PDF se trata de una opción creada por Adobe para poder tener un enlace gráfico a la firma electrónica incrustada en el documento, localizando dicha marca en una posición determinada dentro de una página del documento, de la misma forma que el acceso situado en el panel de firmas desplegable en la franja izquierda del documento.

Por lo tanto, esta marca visible no es la firma electrónica como tal y su alcance es solamente enlazar a la verdadera firma electrónica incluida en el documento y Adobe PDF permite que dicho enlace en forma de marca visible sólo se pueda situar gráficamente en una posición de una sola página dentro del propio documento.

Recaltar que la firma electrónica incrustada en PDF realizada con Xolido® Sign cubre todo el documento (todo el documento está firmado) sin importar que aparezca o no dicha marca visible o la página donde ésta se encuentre.

Mediante las opciones incluidas bajo el epígrafe **Página para incluir la Marca de Firma**, el usuario puede seleccionar entre diversas opciones la página en la que desea que aparezca la información visible de la firma, pudiendo ser la primera, última o cualquier página declarada por el usuario dentro de las dimensiones del PDF.

A través del cuadro de selección **Seleccionar Posición de la Marca de firma**, el usuario puede establecer la posición de la marca de firma en la página seleccionada del documento PDF.

Se ha añadido la opción de *Establecer posición* entre las distintas posibilidades predefinidas, para que el usuario pueda definir y seleccionar sobre una imagen la posición que mejor se adapte a sus necesidades.

Para establecer una posición configurable y manual mediante el botón *Establecer* dentro de la opción **Establecer posición**, el usuario contará con una posible **pre visualización de la página del documento sobre el cual deberá escoger la posición de la marca visible de la firma** mediante el ratón, en un cuadro de diálogo similar al que se muestra en la siguiente imagen.

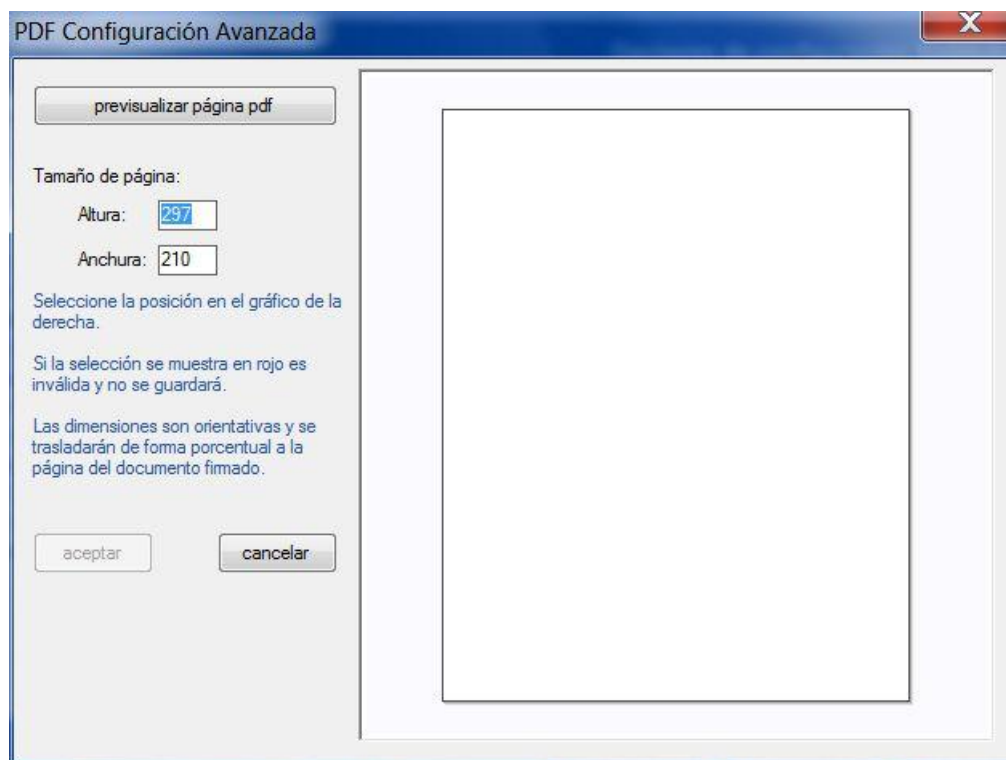


Fig. 31. Selección manual de posición de firma visible PDF.

También se incluye la opción de añadir una **imagen de fondo para la marca de firma** PDF visible, la cual también puede ser configurada en la opción correspondiente del panel y cuyo efecto se

aplicará a los archivos PDF con firma visible que se procesen mientras se encuentre establecida la opción. Ésta imagen de fondo puede ser en formato vectorial WMF que presentará una visualización óptima independientemente del grado de zoom posterior sobre el documento.

Además se permite incluir sólo la imagen de fondo en la marca de firma visible.

Por último, al igual que en los casos anteriores, en todo este grupo de configuraciones se puede **restablecer valores por defecto** para cada panel en caso de querer retornar al estado original de la configuración.

5.5. Zona de Opciones de Salida

El siguiente grupo de configuraciones permite establecer apartados relacionados con la forma y lugar de salida de los archivos operados por la aplicación.

5.5.1 – Carpeta de Salida

En este panel se puede **seleccionar una carpeta de salida** por defecto para los documentos firmados o sellados, y sus firma o sello de tiempo asociado.

Por defecto, viene establecido en la propia aplicación Xolido® Sign, una carpeta dentro del directorio de Documentos del Usuario de Windows, sin embargo esto es configurable de forma que si se establece otra ruta desde este menú, al iniciar la aplicación siempre aparecerá dicha carpeta de salida y no habrá que volverla a seleccionar manualmente antes de iniciar la operación de firma o sello de tiempo de los documentos.

Se puede también desde este menú de configuración, **abrir la carpeta seleccionada** así como **restablecer valores por defecto** incluidos en la aplicación.

Hay que remarcar que al terminar la operación aparecerá en la carpeta de salida el documento que se ha firmado o sellado junto con su firma o sello de tiempo externo asociado, o bien si se trata de documentos PDF y se ha optado por realizar la firma incrustada PDF, el resultado en la carpeta de salida será un archivo PDF con el mismo nombre que el original, pero con la firma digital incrustada en él.

Se muestra a continuación una imagen con el panel de opciones que acabamos de explicar.

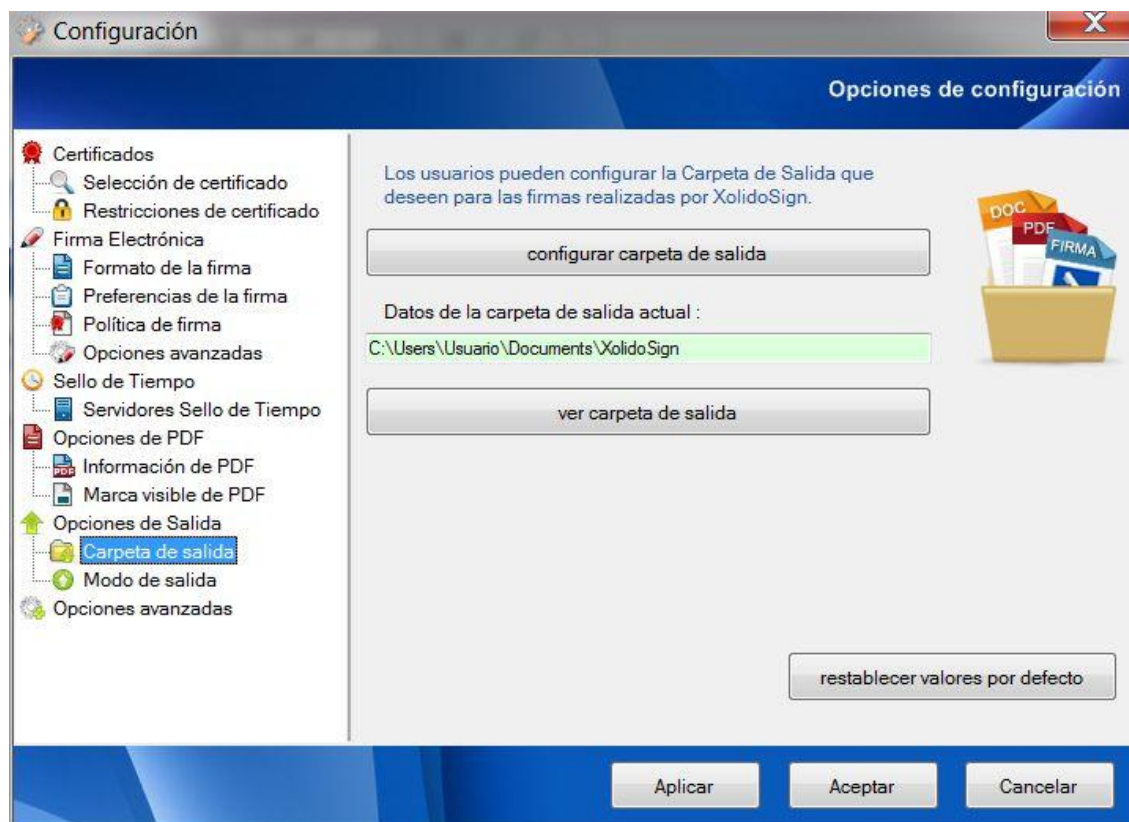


Fig. 32. Carpeta de Salida.

5.5.2 – Modo de Salida

La segunda agrupación de opciones está relacionada con el modo de salida. Se puede establecer el modo en que la aplicación guardará los resultados durante la operación de firma o sellado de tiempo en la carpeta de salida.

Se pueden usar las siguientes opciones:

- *Modo simple*: el archivo se guarda con el nombre original.
- *Modo por defecto*: el archivo se guarda con el nombre original agregando la cadena “_firmado” tras la parte del nombre anterior a la extensión, conservando la extensión original.
- *Modo identificado*: el archivo se guarda con el nombre original agregando, tras la parte del nombre anterior a la extensión, la cadena “_firmado_por_” seguido por el nombre básico del certificado seleccionado y finalizado con la extensión original.
- *Modo carpeta*: Para cada operación de firma, se crea una carpeta con la fecha, hora y un identificador único para la operación de firma conjunta. Dentro, se depositan los archivos en el mismo formato que en el modo identificado

- **Modo personalizado:** Se configura a través de una cadena de texto editable. Por defecto la cadena será igual al último modo no personalizado seleccionado.

La cadena se copia tal cual, con excepción de unos identificadores especiales que se sustituirán durante el proceso de firma. En caso de existir un separador de carpeta (\), la aplicación creará la ruta dinámicamente durante la operación.

Los identificadores especiales son:

- **%n** – Se sustituye por la parte del nombre del archivo anterior a la extensión
- **%x** – Se sustituye por la extensión. Incluye el punto separador.
- **%D**- Se sustituye por la fecha cuando se inicia la operación de firma en grupo. Su formato es año-mes-día.
- **%d**- Se sustituye por la fecha en que se firma el elemento concreto. Su formato es año-mes-día.
- **%H**- Se sustituye por la hora (hora, minuto, segundo) cuando se inicia la operación de firma en grupo. El formato es h00-m00-s00.
- **%h**- Se sustituye por la hora (hora, minuto, segundo) cuando se realiza la firma del elemento. El formato es h00-m00-s00.
- **%I**- Identificador aleatorio único generado para la operación de firma en grupo.
- **%i**- Identificador aleatorio único por cada operación de firma.
- **%N**- Identificador de nombre obtenido a partir del certificado (normalmente el campo CN del asunto del certificado. Si no está disponible, el campo OU, el campo O, o en último lugar, el asunto completo). Se eliminarán o sustituirán algunos caracteres para garantizar que el nombre del archivo será válido para el Sistema Operativo.
- **%S**- El asunto del certificado completo. Se eliminarán o sustituirán algunos caracteres para garantizar que el nombre del archivo será válido para el Sistema Operativo.

Para las operaciones con resultado no incrustado, como es el caso de las firmas de archivos independientes o los sellos de tiempo, se agrega la extensión *.p7b* o *.tsr* a los nombres determinados por el modo de salida escogido.

A continuación se muestra una imagen con las opciones disponibles en la pestaña de configuración del modo de salida.

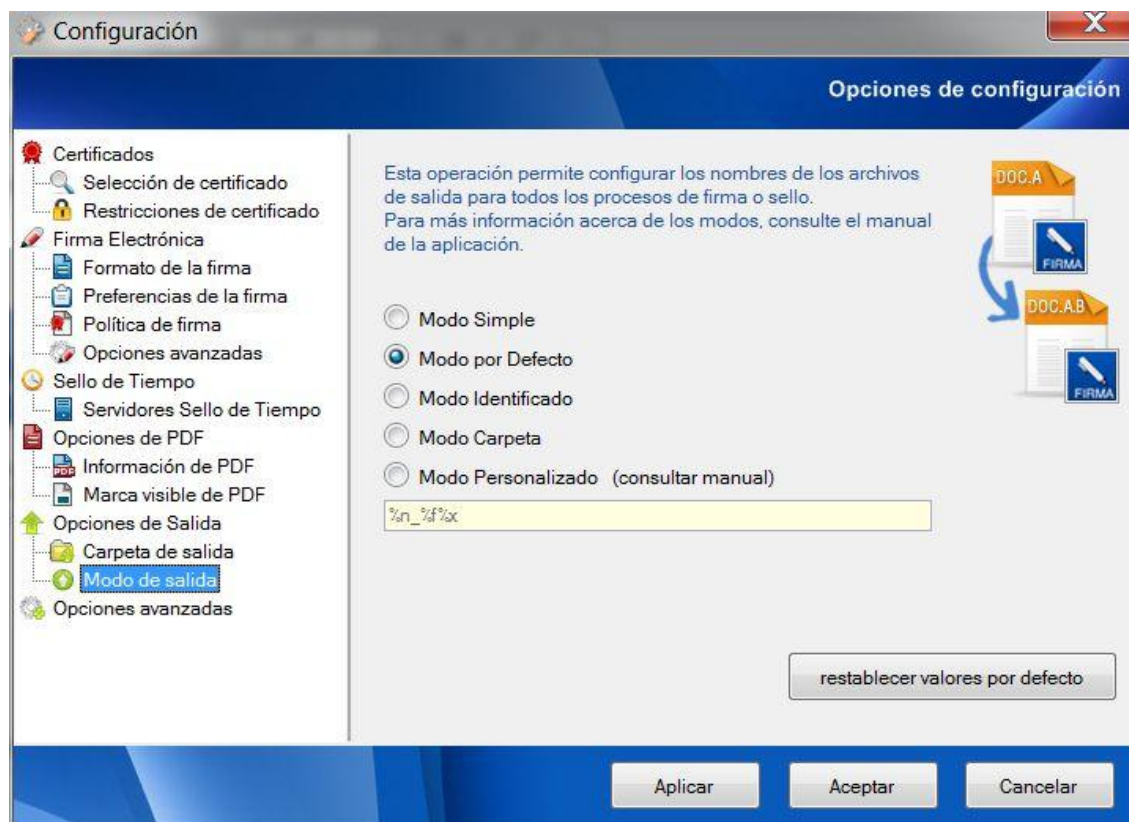


Fig. 33. Modo de Salida.

5.6. Zona de Opciones Avanzadas

El siguiente grupo de opciones tienen un carácter más avanzado y hacen referencia a las dos siguientes funcionalidades:

5.6.1 – Registro de firmas y sellos

En el archivo de Registro de Firmas y Sellos se guardan datos relacionados con las operaciones de firma o sello de tiempo, en formato CSV.

Una vez abierto el archivo de Registro en cualquier aplicación compatible con el formato CSV (por ejemplo Microsoft Excel), el usuario encontrará una tabla con los siguientes datos:

- Identificador del proceso de firma
- Ruta y nombre del archivo original firmado durante el proceso
- HASH correspondiente al proceso de firma
- Fecha de la firma

- Tipo de firma: incrustada para PDF con firma nativa, o formato PKCS7 para firmas externas
- Nombre del certificado empleado para la firma
- HASH correspondiente al certificado empleado para la firma

El usuario puede activar el Registro de Firmas marcando la opción correspondiente, **Activar Registro de Firmas electrónicas y sellos de tiempo en la ruta configurada**.

La ruta para guardar el Registro de Firmas se indicará en el cuadro de texto **Ruta de Registro de Firmas configurada**.

Haciendo click en el botón **restablecer valores por defecto**, el usuario puede recuperar las opciones seleccionadas por defecto en la aplicación.

A continuación se muestra la imagen correspondiente a la pestaña de configuración para éste Registro de Firmas.

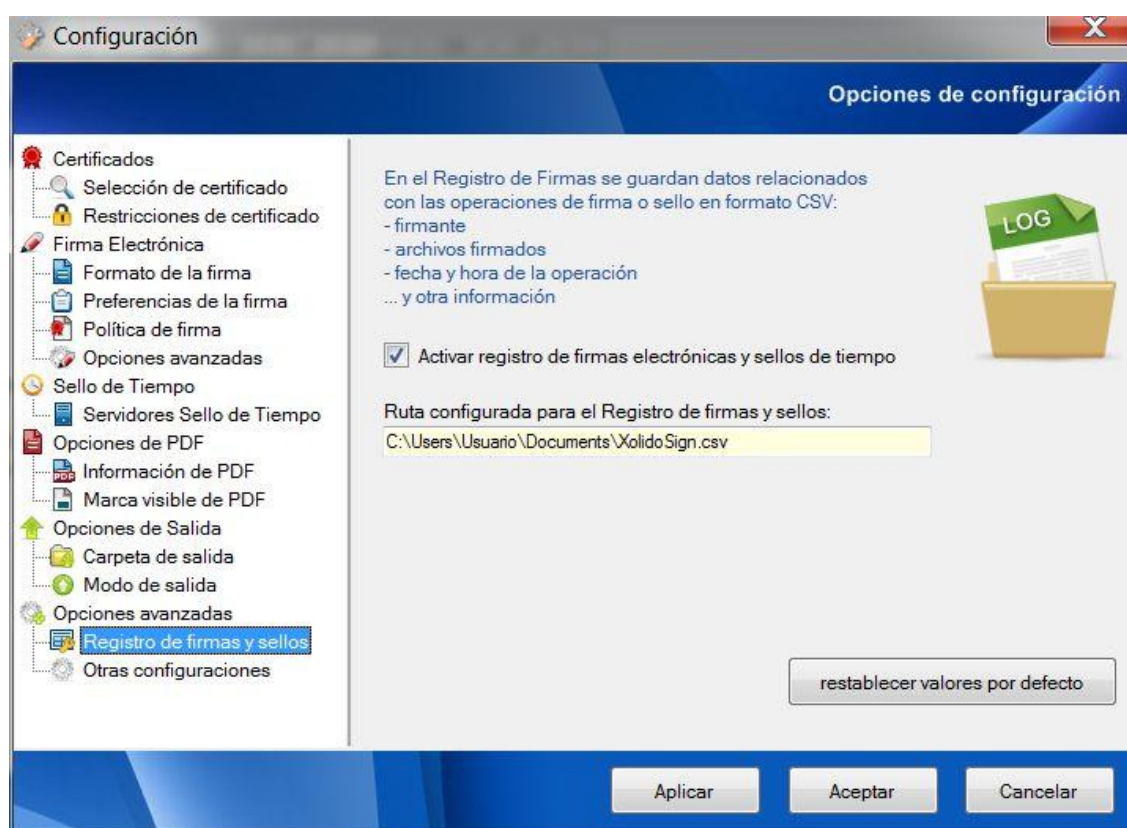


Fig. 34. Registro de Firmas y Sellos.

5.6.2 – Otras configuraciones

El segundo panel de opciones agrupa otras configuraciones, susceptibles de cambio solamente por parte de usuarios con conocimientos específicos o bajo solicitud del servicio de soporte técnico al usuario de Xolido®Sign.

Es recomendable no modificar estas opciones sin tener exacto conocimiento de los cambios que se pretenden conseguir, ya que una incorrecta modificación podría ocasionar problemas en el funcionamiento de la aplicación.

Tenemos la posibilidad de establecer el **tamaño reservado dentro del PDF para la firma incrustada** en dichos documentos. Se puede modificar su valor aunque la aplicación nunca permitirá, por seguridad, un valor inferior a 16.000 Bytes.

En versiones anteriores de Xolido®Sign, este panel contaba con diversas opciones adicionales de configuración general, que ahora pueden accederse a través de las **Opciones Globales del Panel de Control**.

A continuación se muestra la imagen referente al panel de configuración de las opciones avanzadas que se acaban de detallar.

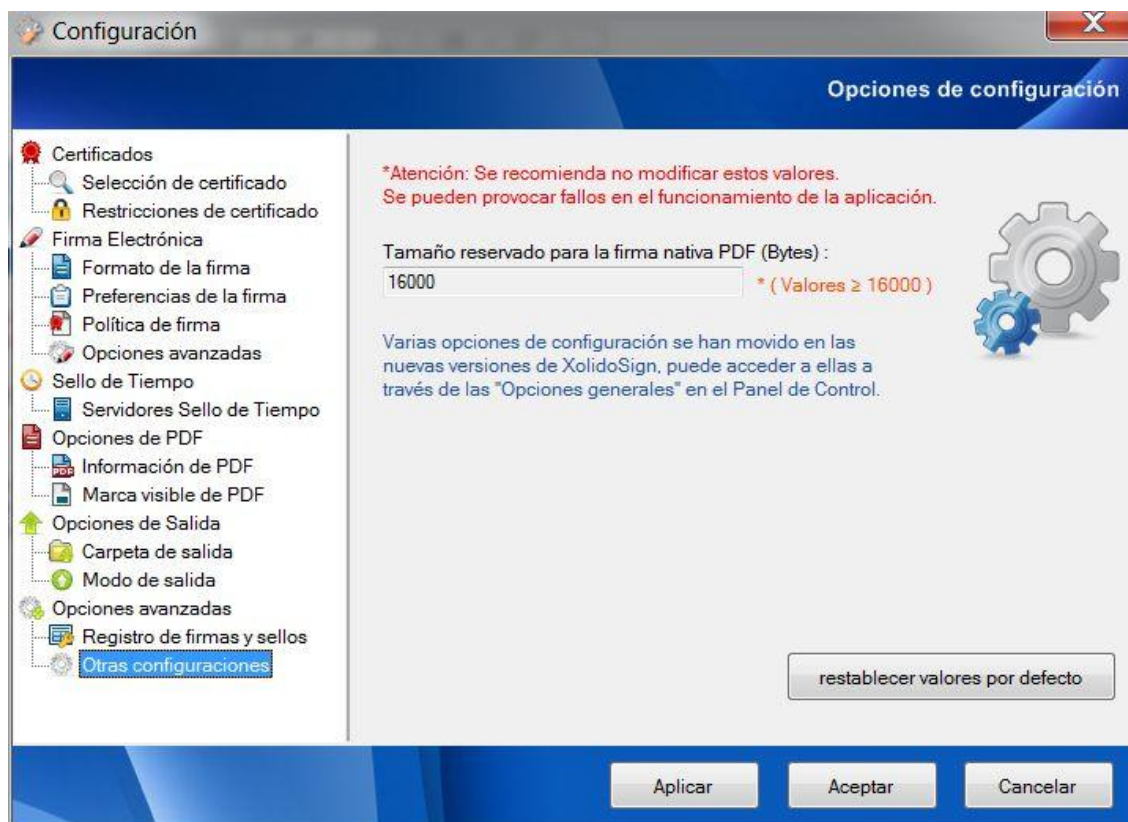


Fig. 35. Otras configuraciones.

6. Uso de la aplicación Xolido®Sign - Verificar



Fig. 36. Cómo usar la aplicación gratuita Xolido®Sign para verificar.

Xolido®Sign permite realizar la verificación electrónica de archivos con firma electrónica y/o con sello de tiempo, garantizando que el documento con el que se ha operado cumple la propiedad de integridad, no ha sido modificado desde su firma o sellado, y asegurando la identidad del autor o firmante.

También verifica las firmas electrónicas externas y/o sellos de tiempo, de forma que trata de asociarles a los correspondientes archivos firmados o sellados, y muestra el resto de información de verificación correspondiente.

El procedimiento de verificación de las firmas electrónicas con Xolido®Sign cumple los estándares de ETSI (www.etsi.org), e IETF (www.ietf.org).

Los formatos de firma electrónica de documentos que Xolido®Sign procesa pueden ser PKCS#7, CMS, firma integrada en PDF (PAdES), CAdES, XMLDsig, XAdES y sellado de tiempo estándar (RFC 3161) y OASIS XML TST. Además las firmas pueden ser con contenido externo o incrustado, lo que comúnmente se conoce como firmas *detached* y *attached* respectivamente.

Así mismo, la aplicación está en constante desarrollo, para la integración de nuevos formatos de verificación soportados.

6.1. Modos de verificación

Xolido®Sign cuenta con dos modos de funcionamiento, verificación inteligente y verificación manual.

Éstos presentan diferencias intrínsecas tanto en la funcionalidad ofrecida como en la forma de proceder a la hora de obtener los resultados.

6.1.1. – Verificación inteligente

El modo de verificación inteligente realiza un proceso automático de emparejamientos y asociaciones entre los archivos y las firmas electrónicas y/o sellos de tiempo incluidos en la lista de selección y proporciona el estado de validez de firmas, sellos y archivos.

Además el sistema trata de encontrar firmas electrónicas y sellos de tiempo asociados a cada uno de los archivos en la misma carpeta donde se localiza el archivo. Las coincidencias se realizan basándose en diferentes mecanismos, como búsqueda por tamaño referenciado en la firma o el nombre del archivo.

Así mismo, para las firmas electrónicas externas y/o sellos de tiempo que no se hayan asociado a ningún archivo, se intentará encontrar los correspondientes archivos firmados o sellados y en todo caso se mostrará también su información de verificación.

Por ello, este modo de funcionamiento está recomendado para su uso habitual, ya que facilita al usuario las tareas de verificación, delegando en la aplicación la búsqueda automática de las correspondencias entre los archivos y sus firmas electrónicas.

En esta modalidad de verificación el usuario tiene que introducir única y exclusivamente un listado de archivos y firmas y/o sellos de tiempo, sin preocuparse de su tipo a la hora de la selección.

Tras ello, haciendo click en el botón de “iniciar operación”, dispondrá de todas las asociaciones procesadas por Xolido® Sign, mostradas de una forma estructurada e intuitiva con el resultado de la verificación de cada uno de los archivos y sus firmantes asociados, bien se correspondan con firmas electrónicas o sellados de tiempo.

A continuación se muestra la interfaz que presenta esta modalidad.

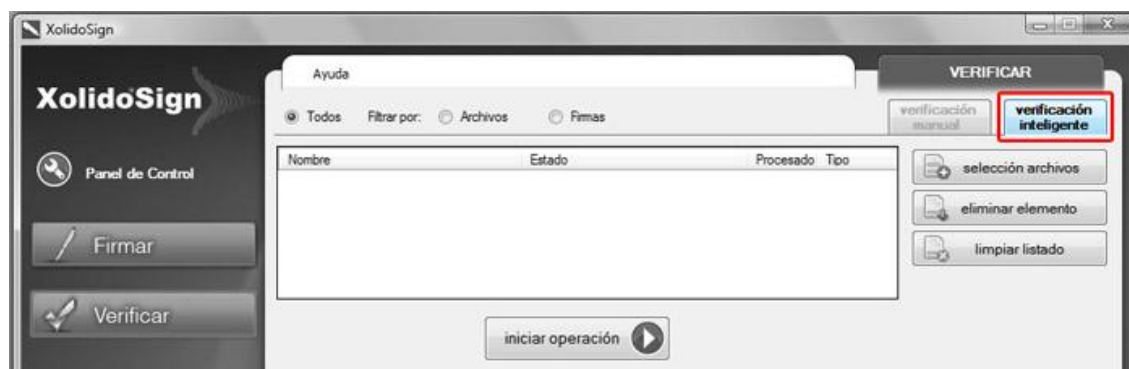


Fig. 37. Interfaz de Verificación Inteligente.

Esta modalidad presenta en la franja superior un filtro para ayudar al usuario en aquellos casos en que disponga una amplia lista de elementos escogidos, pudiendo clasificarlos según se hayan procesado como firmas electrónicas o sellos de tiempo, o bien como archivos y documentos.

6.1.2. – Verificación manual

El modo de verificación manual se emplea cuando el usuario desea contrastar una serie de firmas y/o sellos de tiempo con un archivo concreto, indicando la relación de forma explícita, esto es, preestableciendo cuál es el archivo a verificar y cada una de las firmas y/o sellos de tiempo externos que Xolido® Sign debe contrastar con dicho archivo.

Para ello, la interfaz presenta una primera tabla donde se agregará el elemento que se desea procesar como archivo y una segunda tabla a la cual se pueden ir agregando múltiples elementos que se tratarán de computar como firmas electrónicas o sellados de tiempo y se contrastarán de forma obligatoria con el archivo previamente escogido.

El resultado del proceso muestra el estado de validez de cada uno de los elementos que habiendo sido asociados al archivo se han podido procesar como firmas electrónicas o sellados de tiempo.

A continuación se muestra la imagen de la aplicación con el modo de funcionamiento manual seleccionado.

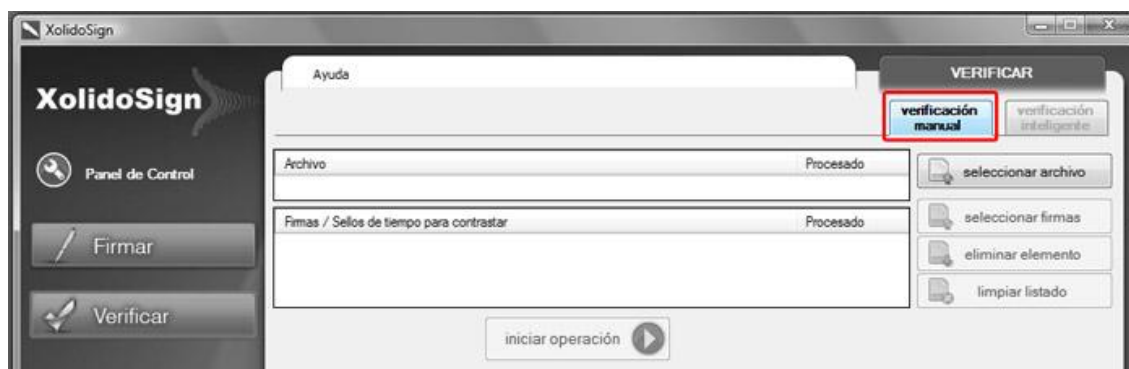


Fig. 38. Interfaz de Verificación Manual.

6.2. Proceso de verificación electrónica

El procedimiento de verificación de archivos firmados electrónicamente y/o sellados de tiempo llevado a cabo por Xolido® Sign incluye como pasos más representativos los siguientes puntos:

- Determinar, para cada uno de los archivos a procesar, la relación de firmas electrónicas y/o sellados de tiempo que se pueden asociar.
- Determinar cada uno de los firmantes implicados en cada una de las firmas electrónicas asociadas a un documento o archivo.
- Comprobar la fecha en la que se realizaron las firmas electrónicas.
- Obtener y validar los certificados electrónicos empleados en el momento de realización de las firmas electrónicas.
- Obtener la información del estado de revocación de los certificados tanto para el instante actual, como en el momento de realización de las firmas electrónicas (mediante mecanismos estándar CRL u OCSP) para comprobar su estado de validez.
- Comprobar la integridad de los datos electrónicos mediante los algoritmos criptográficos reconocidos.
- Extraer los datos completos del firmante y permitir el acceso al certificado digital empleado por el mismo.
- Determinar la fiabilidad que las autoridades de certificación (CA) y autoridades de sellado de tiempo (TSA) merecen, en función de las entidades reconocidas por el usuario, a través de su almacén de autoridades raíz de confianza.

Un punto clave dentro de la verificación electrónica consiste en la comprobación y análisis de los certificados empleados para realizar las firmas electrónicas por parte de los firmantes.

El tiempo empleado por la aplicación para la obtención de los resultados y la finalización de la operación puede variar considerablemente dependiendo de la lentitud o rapidez con que responde cada una de las CA a las peticiones del estado de revocación de sus certificados.

El procedimiento de validación de certificados digitales se describe en el estándar RFC 5055. Entre los pasos ejecutados por Xolido®Sign para el chequeo de certificados se incluye:

- Validar todos los certificados de la cadena de certificación, para determinar el grado de confianza que se puede atribuir al certificado del firmante.
- Comprobar el nivel de confianza de las distintas autoridades de certificación usadas para la comprobación del estado de revocación del certificado.
- Analizar los datos que incluyen los certificados para comprobar su integridad estructural.
- Determinar los datos del propietario del certificado digital.

La verificación de las firmas electrónicas y sellados de tiempo se basa en el grado de bondad de las siguientes características fundamentales, que sirven para determinar el estado global de validez, y son:

- **Confianza**

La aplicación establece que el certificado empleado por el firmante es de confianza cuando se puede construir una cadena de confianza completa y el certificado raíz de ésta se encuentra instalado en el almacén de entidades de confianza de Windows en el ordenador.

Para que la cadena de confianza se pueda completar, Xolido®Sign necesita disponer de todos los certificados de ésta, pudiendo localizarlos tanto en la firma como en el almacén de certificados de Windows en el ordenador.

Xolido®Sign también evaluará la validez temporal de los certificados y sus propósitos.

- **Revocación**

Las entidades de certificación, CA, utilizan protocolos online para poder informar a los verificadores acerca de la invalidez de sus certificados emitidos, antes de su fecha de caducidad.

Xolido®Sign considera importante la obtención del estado de revocación, ya que es la única manera de garantizar completamente que el certificado empleado para la firma se considera válido en el momento de la firma.

Xolido®Sign indicará una advertencia si no puede obtener la información de revocación e indicará invalidez si obtuviera la confirmación de que el certificado empleado fue revocado con anterioridad a la firma.

En el caso de firmas con datos de revocación incrustados, Xolido®Sign aceptará los valores incrustados si su evaluación se considera correcta. En caso de no poder completarse satisfactoriamente esta evaluación, se realizará una comprobación online de forma convencional.

- **Integridad**

Las firmas electrónicas contienen mecanismos internos que deben ser respetados para que sean criptográficamente válidas.

Xolido®Sign marcará como incorrecta la integridad si alguno de los mecanismos no fuera satisfecho.

- **Correspondencia**

En este apartado Xolido®Sign notifica si los datos firmados coinciden con el archivo que se ha asociado en ese momento. Si Xolido®Sign notificara invalidez podría deberse a que el archivo asociado no es el archivo firmado, o que el archivo firmado fue modificado en posterioridad a la firma.

Además Xolido®Sign puede notificar un estado inválido si no se hubiera encontrado una asociación con un archivo firmado. Si éste fuera el caso, posteriormente se permitirá al usuario que busque y seleccione el archivo manualmente.

- **Momento de la firma**

Uno de los aspectos más importantes, dentro del contexto de las firmas electrónicas, es conocer el instante de tiempo en que se realiza la firma.

El momento de la firma es vital para conocer la validez y estado de revocación de los certificados electrónicos empleados en el proceso de firma electrónica y por tanto su importancia trasciende a un nivel que llega a conceder o denegar la confianza en todo el proceso de firma electrónica.

Para garantizar este dato existen varios mecanismos, cada uno de los cuales está asociado a un nivel de confianza y credibilidad, Xolido®Sign computa para todas las firmas electrónicas procesadas

el momento de su creación y determina un grado de prioridad en caso de existir varias fuentes de tiempo.

En primer lugar, se considera el caso de que la firma incluya un sellado de tiempo proporcionado por una autoridad de sello de tiempo (TSA) de confianza. En este supuesto, la fecha y hora que anuncia dicha entidad tercera en confianza es asumida como el momento de creación de la firma electrónica.

En caso de no incluirse un sello de tiempo de la firma, el firmante puede haber incluido, en el momento de su realización un atributo estándar que indica la fecha y hora de creación declarada. Al tratarse de un valor que determina el propio firmante, Xolido®Sign mostrará dicho instante de tiempo a modo informativo pero no lo acepta como fecha confiable.

En el caso de las firmas integradas en documentos PDF, y que no incluyan sello de tiempo, el propio documento contiene unas estructuras con información, entre otras cosas, acerca del instante de creación de la firma electrónica. Xolido®Sign mostrará dicho momento a modo informativo pero tampoco lo acepta como fecha confiable por tratarse de tiempos que proceden del ordenador del firmante y por ello, pueden ser fácilmente manipulables.

6.3. Resultados de verificación

A partir de los datos obtenidos a lo largo del proceso de verificación Xolido®Sign presenta los resultados en un formato entendible y tratando de minimizar la complejidad subyacente a la hora de mostrar la información, de forma que los usuarios puedan tener una idea global y completa acerca del estado de validez de cada una de las firmas o sellos de tiempo asociados a los archivos tratados por la aplicación.

En todos los casos, se presenta el resumen correspondiente a los resultados obtenidos para cada uno de los puntos clave que se deben analizar en el proceso de verificación electrónica, tal y como hemos comentado en el punto anterior.

La aplicación dispone de dos interfaces de presentación de los datos, archivos y firmas electrónicas / sellos de tiempo, diferenciadas según el tipo de procesado que haya recibido cada uno de los elementos. Estas interfaces se exponen a continuación.

6.3.1. – Archivos

Cuando el elemento se procesa como archivo, aparecerá el resumen que se muestra en la imagen a continuación.



Fig. 39. Resultado de Verificación de Archivo.

Se pueden distinguir varias zonas, la parte superior indica el nombre y ruta de acceso al archivo, junto con el botón “**ver archivo**” para poder abrirlo directamente desde Xolido® Sign (en caso de que el sistema operativo disponga de una aplicación asociada).

A continuación se muestra un listado de cada uno de los firmantes asociados al archivo.

Mediante una leyenda de color se indica la procedencia de cada una de las firmas en las que se encuentra el firmante mostrado, pudiendo ser un elemento existente en la selección del usuario, o uno que proceda de la búsqueda extendida realizada por la aplicación en la verificación inteligente, o bien una firma incrustada en el propio archivo (para el caso de las firmas integradas en PDF), o un elemento que el usuario ha enlazado manualmente con un archivo, dentro de la verificación manual.

La siguiente zona del panel de información muestra el resultado de la verificación para el firmante seleccionado.

Tal y como se ha expuesto previamente, Xolido® Sign considera varios puntos de especial interés en el cómputo de una verificación. Éstos apartados son los que se presentan en el panel, con un código de color de fondo, que indica su grado de validez de forma intuitiva.

Además de presentarse la información de cada uno de los apartados relativos a la verificación electrónica, Xolido®Sign realiza una valoración global del estado asociado a cada uno de los firmantes, y lo indica mediante un icono al lado del nombre del firmante.

Los iconos de dicha valoración y su significado se muestran a continuación.

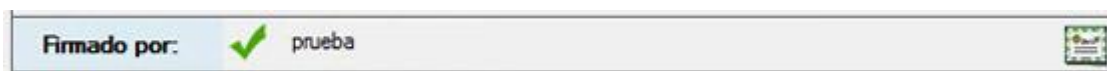


Fig. 40. La firma es válida.

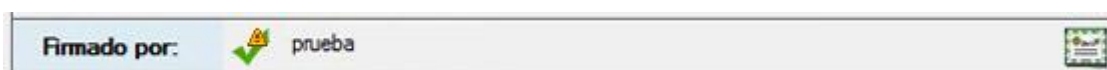


Fig. 41. La firma es correcta pero deberían revisarse las advertencias.



Fig. 42. La firma presenta problemas.

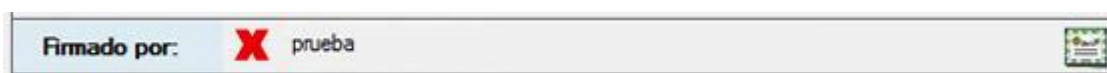


Fig. 43. La firma no es válida.

De esta forma, si el usuario se desplaza a lo largo de todos los firmantes asociados al archivo y mostrados en la lista, puede visualizar rápidamente, para un archivo dado, su estado de validez de acuerdo a la información criptográfica asociada, analizando la confiabilidad de sus firmas electrónicas y/o sellos de tiempo.

Presenta un botón, denominado **"ver informe"** en la posición inferior derecha, para acceder al informe extendido de verificación de la firma seleccionada en ese momento.

Dicho informe contiene la información precisa acerca de las variaciones y eventos que se producen en cada uno de los casos de verificación, de forma que los usuarios más avanzados pueden consultar el análisis completo de los resultados obtenidos por Xolido®Sign.

Se emplea en todo caso un código de color y simbología básica e intuitiva para que los usuarios puedan percibir de forma sencilla el resultado de la verificación.

6.3.2. – Firmas electrónicas / Sellos de Tiempo

Para los elementos procesados como firmas electrónicas y sellos de tiempo, aparecerá el resultado mostrado en la imagen a continuación.

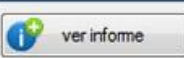


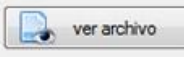
Firma digital	
Nombre:	prueba.p7b
Directorio:	C:\Users\Usuario\Desktop
	
Firmado por:	 prueba 
Avalado por:	Root Agency
Confianza:	Firmante de confianza.
Revocación:	El certificado firmante no está revocado.
Integridad:	Estructura de firma correcta.
Formato:	PKCS7 / CAdES-T
Fecha	
Sello de Tiempo	
05/08/2010 13:37:06	
Archivo asociado	
C:\Users\Usuario\Desktop\prueba.txt	
Correspondencia:	La firma se corresponde con el archivo.
	

Fig. 44. Resultado de Verificación de Firmas Electrónicas y Sellos de Tiempo.

En la zona superior se encuentra la información genérica, su nombre y la ruta en la que se encuentra el archivo de firma electrónica y/o sellado de tiempo, así como el botón **“ver informe”**, para acceder al reporte detallado con el resultado de la verificación para la firma o sello en cuestión. Dicho informe presenta a los usuarios avanzados una información completa y concisa acerca de cada uno de los incidentes que pudieran ocurrir durante el proceso de verificación.

Se presenta un panel para informar de las situaciones en que una firma contenga varios firmantes, lo que se conoce como CoSign, de forma que los usuarios de Xolido® Sign pueden navegar a través de dichos firmantes de manera sencilla, visualizando el estado de validez asociado a cada uno de ellos mediante los iconos de valoración global utilizados por Xolido® Sign (ver Fig.28-31).

Para los firmantes de cada firma se muestra cada uno de los apartados que conforman la información básica de verificación, confianza, revocación, integridad, correspondencia y momento de la firma en paneles con códigos de color intuitivos para que los usuarios interpreten fácilmente los resultados.

En la zona inferior se muestra el apartado referente al archivo asociado a dicha firma electrónica o sello de tiempo, indicando tanto la ruta del archivo en cuestión como el estado de la correspondencia entre archivo y firma o sello.

Además en el botón **“ver archivo”** se puede acceder a él directamente (siempre que el sistema operativo tenga un programa asociado a la extensión).

Incluso para las firmas cuyo contenido firmado está incluido dentro de la propia estructura de firma (attached), la aplicación trata de extraer dicho contenido para poder mostrarlo al usuario de una forma cómoda y sencilla.

6.3.3. – Informe extendido de verificación

Para los usuarios avanzados, o aquellos que deseen consultar una información detallada de cada uno de los apartados que componen la verificación de una firma electrónica o sello de tiempo, Xolido® Sign dispone de un panel de informe de verificación.

Dicho informe tiene un aspecto similar al indicado en la siguiente imagen.

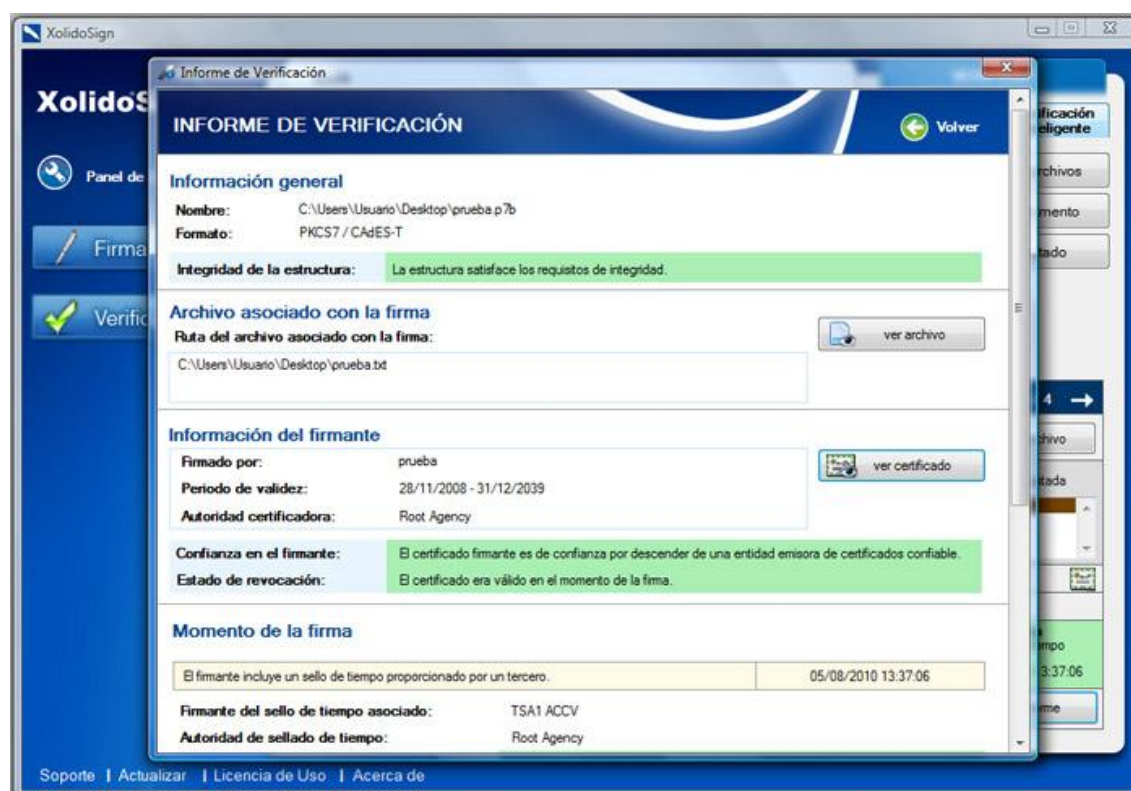


Fig. 45. Informe extendido de Verificación.

En este informe se muestran los datos procesados por Xolido® Sign en el proceso de verificación. Cuenta con apartados extendidos referentes a cada uno de los análisis realizados, entre los que cabe destacar:

- información general acerca del nombre y ubicación en el ordenador del usuario de los archivos tratados durante el proceso, indicando además para la firma su formato, de manera que el usuario puede conocer si el elemento tratado se ajusta a un estándar determinado.
- información acerca del número de firmantes, en caso de tratarse de una firma con CoSign, indicando para cada uno de ellos su nombre descriptivo.
- información completa de cada uno de los firmantes, extrayendo su nombre, autoridad que lo avala, caducidad... y mostrando al usuario los datos extendidos acerca de su estado de confianza y revocación, con las explicaciones pertinentes en cada caso si se han detectado problemas. También se da acceso al usuario al certificado empleado por el firmante, a través del icono correspondiente.
- información acerca del instante de tiempo en que se ha realizado la firma, indicando las diversas fuentes de fecha y hora, si las hubiera. Además, en caso de tratarse de un momento que procede de un sello de tiempo, se completará con la información referente a la autoridad de sellado de tiempo (TSA), y sus correspondientes informaciones de confianza, revocación e integridad, para que el usuario no tenga dudas acerca del grado de validez del instante temporal anunciado para la creación de la firma electrónica.
- información extendida acerca de la integridad de la estructura de firma electrónica y/o sello de tiempo.
- información de la correspondencia de la firma procesada con el archivo asociado, de manera que no sólo se presenta una breve explicación, sino también aparecerán el resumen firmado (desencriptado a partir de la propia firma o sello) y el resumen del archivo asociado.

7. Información técnica adicional de Xolido®Sign

Xolido®Sign dispone de información para los usuarios más avanzados en temas técnicos.

Entre los datos adicionales que se desarrollan en la aplicación se encuentra un control más exhaustivo de la información de revocación para los certificados firmantes. Xolido®Sign dispone de su propio espacio de nombres dentro del árbol de identificadores (OID) que la entidad internacional IANA (*Internet Assigned Numbers Authority* - www.iana.org) facilita para el establecimiento de estructuras informativas de nivel esencialmente técnico, partiendo del identificador raíz (1..3.6.1.4.1.35788) asignado a Xolido Systems, S.A.

La documentación referente a dichas estructuras de datos en árbol que Xolido®Sign emplea para ofrecer a los usuarios un control más riguroso y exhaustivo de sus firmas electrónicas se dispone dentro de la carpeta **DOC** en el directorio de la aplicación, con el nombre *XolidoSign Información Técnica*. Éste documento sólo se proporciona en español.

Así mismo, Xolido®Sign proporciona a los usuarios un registro de cambios llevados a cabo en la aplicación a lo largo de su historial de versiones. Ésta información puede ser interesante para conocer las mejoras y nuevas funcionalidades añadidas con el paso del tiempo en la aplicación. Dicho archivo se llama *Changelog* y se localiza dentro de la carpeta **DOC** en el directorio de la aplicación. Ésta información sólo se proporciona en español.

También se proporciona en dicha carpeta **DOC** los archivos de manual de usuario en PDF, tanto en la versión en español como en inglés.

8. Otra información acerca de Xolido® Sign

La aplicación cuenta con una ayuda offline estructurada, que además contiene información acerca de los conceptos de firma digital y sello electrónico temporal, y que puede ser consultada a través del menú superior de la aplicación, siguiendo la ruta *Ayuda -> Ayuda* o bien presionando la tecla *F1* de su teclado.

La aplicación también realiza un control silencioso de la existencia de nuevas versiones para que el usuario de Xolido®Sign pueda estar al día en cuanto a la versión utilizada y pueda disfrutar de los nuevos avances que contengan las versiones más modernas de la aplicación.

Xolido®Sign dispone, de forma gratuita para todos los usuarios que lo deseen, de la posibilidad de suscribirse a una lista de correo para poder recibir las últimas novedades al respecto de la aplicación..

La dirección desde la que usted puede suscribirse a la lista de correo es la siguiente: [Suscripción a Lista de Correo Xolido® Sign](#)

(<http://www.xolido.com/products/xolidosign/news/subscribe/>).

Cualquier sugerencia al respecto de posibles mejoras en la aplicación, o dudas e relación a su funcionamiento o uso pueden hacerlas llegar a través de la dirección de correo xs@xolido.com.

© 2001-2017 Xolido Systems, S.A.

Todos los derechos reservados.

Xolido® es una marca registrada.

Este documento es propiedad de Xolido Systems, S.A.

El contenido de este manual se proporciona únicamente con fines informativos y podrá ser modificado sin previo aviso por parte de Xolido Systems, S.A.

Xolido Systems, S.A. no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.