Firma Digital

Manual para SAS de Ciudad Autónoma de Buenos Aires

Versión 2.0 - 03/2019

Inspección General de Justicia

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

Introducción

¿Qué es?

La firma digital es una solución tecnológica que permite ***añadir*** a documentos digitales y mensajes de correo electrónico una ***huella o marca*** única, a través de ciertas operaciones matemáticas.
La firma digital permite al receptor del mensaje o documento:

- Identificar al firmante de forma fehaciente (***Autenticación***)
- Asegurar que el contenido no pudo ser modificado luego de la firma sin dejar evidencia de la alteración (***Integridad***)
- Tener garantías de que la firma se realizó bajo el control absoluto del firmante (***Exclusividad***)
- Demostrar el origen de la firma y la integridad del mensaje ante terceros, de modo que el firmante no pueda negar o repudiar su existencia o autoría (***No Repudio***)

Conforme la Ley 25.506, la firma digital cumple las ***mismas exigencias*** que la firma manuscrita de los documentos en papel, ya que posee las mismas características técnicas de seguridad que una firma en papel, e incluso mayores.

¿Para qué sirve?

Facilita el reemplazo de documentación en papel por su equivalente en formato digital. Ahorra costos, simplifica procedimientos y brinda seguridad en el intercambio de información.

Se utiliza principalmente para firmar documentos PDF y correos electrónicos, pero también permite firmar documentos de texto, plantillas, imágenes y virtualmente cualquier tipo de documento. Su tecnología está incorporada en transacciones electrónicas, formularios web y navegación en páginas seguras.

¿Cómo funciona?

La tecnología de firma digital se sostiene de dos pilares: un método que hace imposible la alteración de la firma y una infraestructura que permite certificar la identidad del firmante.

Clave Asimétrica

La Clave Asimétrica es un método de criptografía o codificación, en el que se generan dos números de gran longitud (usualmente más de 200 cifras) mediante una fórmula matemática compleja. Estos números, llamados "claves", son distintos, pero están relacionados de modo tal que ***lo que se cifra o encripta con una clave sólo puede descifrarse con la otra***. A este par de claves se los conoce como ***Clave Pública*** y ***Clave Privada***. La clave pública se distribuye y la clave privada la conserva el propietario, protegida por una o varias contraseñas que sólo él conoce. El par de claves funciona siempre en conjunto: No es posible cifrar y descifrar un documento con una misma clave.
Cuando se aplica la clave privada sobre un documento digital en su totalidad, este queda cifrado o encriptado. Es decir, se vuelve ilegible para cualquiera que no posea la clave pública con que descifrarlo. En firma digital, ya que no se busca encriptar el mensaje sino darle una marca de autenticación, la clave asimétrica se utiliza de forma indirecta, no sobre el documento, sino sobre un resumen del mismo, denominado hash.

Hash

El hash (también conocido como digesto o huella digital), es un resumen único que identifica a un documento digital. Se puede aplicar a cualquier tipo de documento, incluso a una cadena de texto. Se obtiene al aplicar una fórmula matemática llamada ***"función unidireccional de resumen"***, o función hash. El resultado suele expresarse en números y letras minúsculas de la "a" a la "f" (sistema hexadecimal). Un ejemplo de hash podría ser:
`165d5f1615a80bf0e106df3954c5a73439f659cf02d6c2eb760c21076fb17043`

- Es un ***resumen***, porque sin importar el tamaño del documento, la función devuelve un hash de la misma longitud.
- Es ***unidireccional***, porque no es posible convertir el hash nuevamente en el documento original, ni conocer el contenido del documento a partir del hash.
- Al ser una ***función matemática***, aplicarla sobre un ***mismo documento*** o mensaje devuelve ***siempre el mismo hash***.
- Es estadísticamente ***imposible*** encontrar dos documentos distintos que posean el mismo hash.
- Dos documentos pueden parecer a ***simple vista*** idénticos, pero poseer distinto hash. Aunque parezcan idénticos, si el hash difiere, ***no pueden*** considerarse el mismo documento digital.

Firma

Existe una gran variedad de aplicaciones para firmar digitalmente, pero en esencia todas funcionan del mismo modo:

1. Al momento de firmar, la aplicación calcula el hash del documento.
2. Luego utiliza la clave privada para cifrar ese hash (es en ese momento cuando solicita la contraseña con la que el usuario protegió su clave privada)
3. Finalmente, el hash cifrado se incorpora, junto con otros datos (fecha y hora de firma, datos del firmante, etc), como anexo del documento, obteniendo así un documento firmado digitalmente.

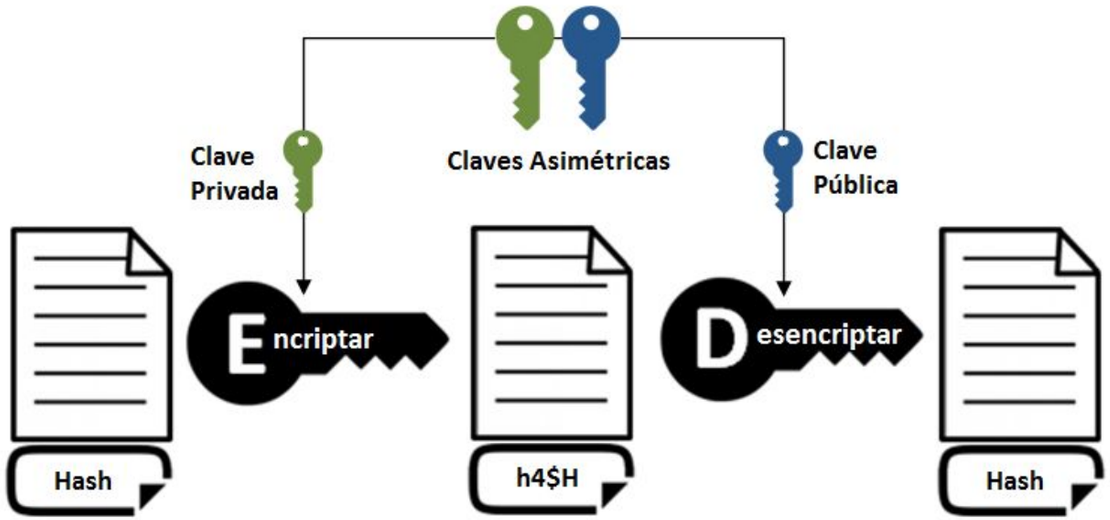
Autenticación

Cualquiera receptor del documento que posea la clave pública puede autenticarlo. Para ello solo debe:

1. Calcular el hash del documento.
2. Descifrar el hash contenido en la firma digital.
3. Compararlos.

Sí los hash coinciden, el receptor puede confirmar dos cosas:

- El contenido del documento no fue alterado luego de la firma,
- la clave privada con que se firmó coincide con la clave pública.



Certificado Digital

Para que el procedimiento de firma y autenticación sea confiable, necesitamos la seguridad de que esa clave pública efectivamente pertenece al firmante. Por eso, el segundo elemento que sostiene el sistema de firma digital es la "Infraestructura de Clave Pública" (PKI, en inglés), que regula cómo se emiten y distribuyen las claves. Para esto, utilizan documentos llamados Certificados de Clave Pública, o según nuestra normativa, Certificados Digitales. Un ***Certificado Digital*** es simplemente un documento firmado digitalmente por una autoridad, en el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene datos de identidad de la persona, su clave pública y el nombre de la autoridad que emitió el certificado. Todos los datos de identidad son previamente validados por esta autoridad, y el certificado se puede autenticar de la misma forma que cualquier otro documento con firma digital.

La Infraestructura de Clave Pública es el conjunto de procedimientos, políticas y roles normados que definen cómo se generan y organizan esos certificados. Si el certificado es auténtico y confiamos en la autoridad emisora, podemos asegurar la identidad del firmante. En nuestro país, esta regulación se conoce como ***Infraestructura de Firma Digital de la República Argentina (IFDRA)***.

¿Quién la regula?

La ***Autoridad de Aplicación*** establecida en la Ley N° 25.506 de Firma Digital. Actualmente el rol lo desempeña la ***SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN*** (SGM) de la JEFATURA DE GABINETE DE MINISTROS. Actúa como ***Ente Licenciante***, otorgando, denegando o revocando las licencias de los Certificadores Licenciados.

La ***Autoridad Certificante Raíz*** (AC-RAÍZ), operada por el Ente Licenciante, es el primer nivel de jerarquía en la IFDRA. Emite certificados digitales a las Autoridades Certificantes de segundo nivel, una vez aprobados los requisitos de licenciamiento.

Los ***Certificadores Licenciados*** son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante para emitir certificados digitales a personas. Estos operan cada ***Autoridad Certificante*** de *segundo nivel*.
Cada Certificador Licenciado delega en ***Autoridades de Registro*** las funciones de validación de identidad y otros datos de los suscriptores de certificados.

¿Cómo la obtengo?

Firma Digital Token: Requiere un dispositivo físico donde se almacena el certificado. Puede verificar los requisitos para obtener un Certificado de Firma Digital Token, y dirigirse ante cualquier Autoridad de Registro de la Administración Pública, o consultar con alguno de los Certificadores Licenciados.

Firma Digital Cloud: Permite firmar a través de una plataforma online. Puede consultar características, requisitos y forma de obtenerla en la Plataforma de Firma Digital Remota (PFDR).

Validación de Firma

Cómo Reconocer una Firma Digital

La firma digital es un pequeño bloque de información que suele anexarse o "incrustarse" al documento firmado. No es directamente visible en el documento, pero la mayoría de las aplicaciones que trabajan con documentos permiten distinguir cuales están firmados y ver los detalles de la firma. Muchos documentos poseen además un ***sello*** o ***marca de agua*** en el texto, que indica datos del firmante o emula la firma manuscrita. Este sello puede ayudarnos a distinguir un documento firmado, pero el sello y la firma digital ***no son lo mismo***: Un documento firmado digitalmente puede carecer de sello, y puede existir un documento sellado sin firma digital.

Diferencia entre Firma Electrónica y Firma Digital

La ley define a la firma electrónica como "*al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital*". Entonces, para poder ser considerada firma electrónica, el procedimiento debe al menos poseer las propiedades de Autenticación e Integridad, y por ende No Repudio. La diferencia entre una Firma Digital y una Firma Electrónica es que la primera se realiza con un Certificado Válido. Los ejemplos más comunes de firma electrónica son:

- Las firmas realizadas con certificados que ***no fueron emitidos por un Certificador Licenciado***, incluyendo
    - certificados emitidos por autoridad certificante ***extranjera*** (salvo las que cumplan los requisitos del art. 16 ley 25.506),
    - certificados emitidos por un ente nacional, privado o público ***sin licencia***,
    - certificados generados ***por el propio firmante*** mediante alguna aplicación informática.
- La firma realizada con certificado válido (emitido por un Certificador Licenciado) pero ***expirado o revocado*** antes de firmar.
- Las firmas de documentos generados mediante las plataformas de ***Trámites a Distancia*** (TAD) y GDE, salvo los casos en que al firmar se haya utilizado un ***Token*** o ***Firma Remota***.

Conforme la ley, la firma electrónica tiene valor legal, pero no tiene el mismo valor de prueba que la firma digital. Si alguien niega o desconoce una firma digital, esa persona tiene que probar que la firma es falsa. En cambio, si alguien niega o desconoce una firma electrónica, es la otra parte quién debe que probar que la firma es auténtica. Si la Firma Digital es comparable a la Firma Certificada en papel, la Firma Electrónica lo es a la Firma Simple. Cuando una norma u organismo exija firma digital, no es suficiente la firma electrónica.

Jerarquía de Certificados

Tal como se menciona en el apartado de Certificados Digitales, todos los certificados emitidos a personas están firmados por una Autoridad Certificante. ¿Pero cómo puedo saber si esa firma es realmente de la autoridad? Por este motivo es que también existen certificados digitales de estas autoridades, los cuales son firmados a su vez por una entidad de mayor jerarquía. Se genera así una "***cadena de confianza***" en la que con sólo adquirir el certificado de la autoridad máxima de manera segura, podremos validar sucesivamente los certificados de menor jerarquía. Conforme la Infraestructura de Firma Digital Argentina, existen dos niveles de autoridad:

1° - Autoridad Certificante Raíz - AC-RAÍZ

Es la autoridad operada por el Ente Licenciante, y por lo tanto, la de mayor jerarquía. Sus certificados son básicos para poder validar cualquier firma digital, y se conocen como Certificados Raíz. Los certificados raíz están firmados por la propia autoridad.

- Certificado AC-RAIZ RA 2007 (necesario para validar Firmas Digitales Token)
- Certificado AC-RAIZ RA V2 (necesario para validar Firmas Digitales Cloud)

2° - Certificadores Licenciados

Son todos aquellos que el Ente Licenciante habilitó a emitir certificados digitales para personas. Se consideran Autoridades Certificantes de segundo nivel, y sus certificados se conocen como Certificados Intermedios. Cada uno de estos certificados es necesario para validar las firmas de todas aquellas personas que hayan adquirido la firma digital con ellos.

- Certificado Autoridad Certificante ONTI (para firmas adquiridas en el Ministerio de Producción y diversos entes públicos)
- Certificado Autoridad Certificante AFIP y AFIP V2, emitido 12/12/18 (para firmas adquiridas ante AFIP)
- Certificado Autoridad Certificante Modernización PFDR (para firmas Cloud, de la Plataforma de Firma Digital Remota - PFDR)

Se enumeran aquí los principales certificados utilizados en la Administración Pública Nacional. En caso de necesitar validar otros documentos, el listado completo de Certificadores Licenciados se encuentra en la página de Firma Digital Argentina: https://www.acraiz.gob.ar/Home/CertificadoresLicenciados

Aún en aquellos casos en que el emisor de un certificado no fuera una autoridad reconocida, es posible adquirir los certificados intermedios del emisor e instalarlos. Eso permitirá validar los documentos firmados con certificados provistos por ese emisor. Esto no es recomendable salvo que se confíe plenamente en la idoneidad del emisor, y aún en estos casos, debe tenerse en cuenta que la firma de dicho documento puede no ser reconocida por terceros, ya que se considera firma electrónica.

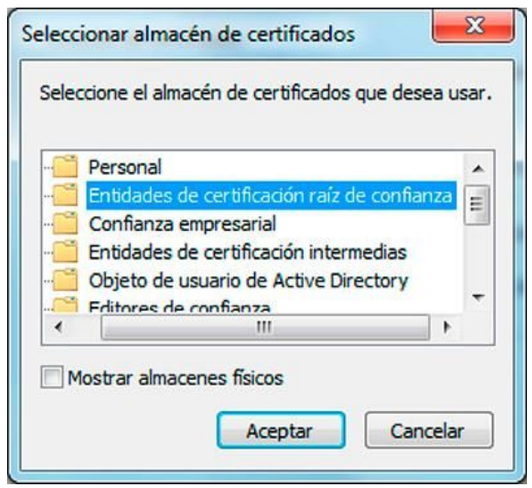
Instalación de Certificados AC

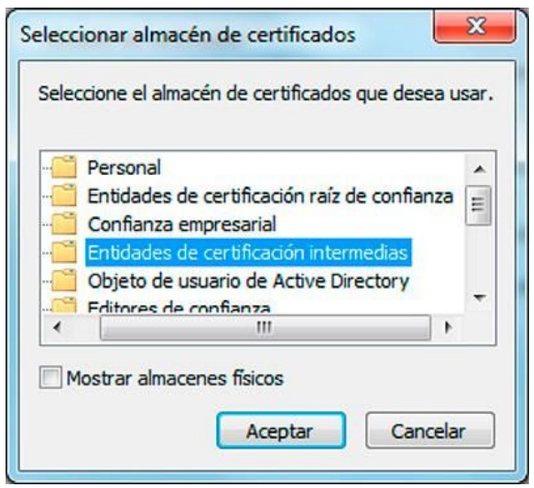
Como paso previo a realizar la verificación de una firma digital, el equipo o dispositivo debe tener correctamente instalados los certificados raíz e intermedios. ***Nota:*** *Para instalar el certificado AC se recomienda haber iniciado una sesión con un usuario con permisos de administrador en su PC.*

1. Descargar el archivo de certificado.
2. Una vez finalizada la descarga, abrir el archivo haciendo doble clic.
    a. Si apareciera una advertencia de seguridad, seleccionar “Abrir”
3. En la ventana de información, hacer click en “Instalar certificado”.

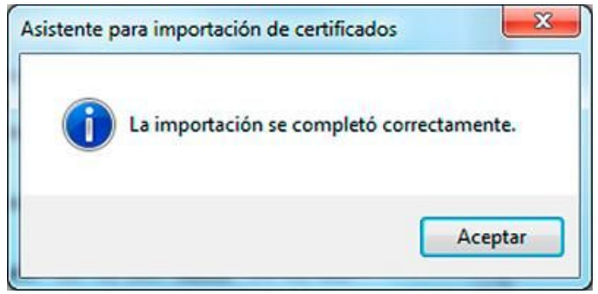
4. Una vez abierto el Asistente para importación de certificados, hacer click en “Siguiente”.
5. Seleccionar la opción “Colocar todos los certificados en el siguiente almacén” y hacer clic en “Examinar”.
6. Seleccionar el almacén de certificados que corresponda con el nivel:

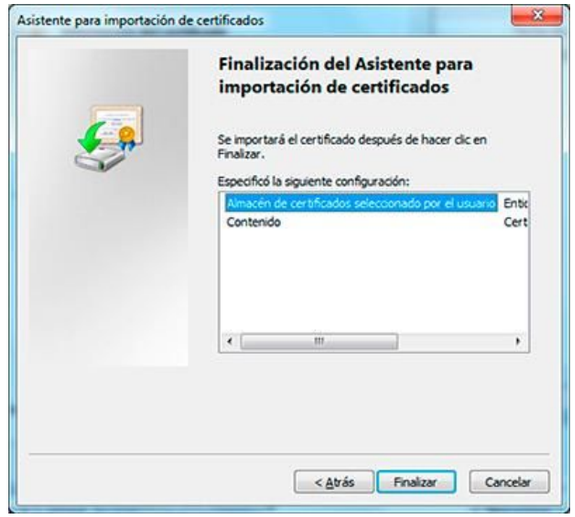
   a. Sí es un Certificado Raíz, seleccionar la carpeta “Entidades de certificación raíz de confianza”
   b. Sí es un Certificado Intermedio, seleccionar la carpeta “Entidades de certificación intermedias”





7. Hacer click en “Siguiente” y luego “Finalizar”.
8. Si el certificado se importó con éxito, debería aparecer la ventana final indicándolo.





Todos los certificados instalados pueden consultarse ingresando desde Windows al Panel de Control>Opciones de Internet>Contenido>Certificados. Además de los certificados instalados manualmente, se verán todos los que el sistema operativo instala de manera predeterminada.

Vigencia de los Certificados

Cuando una autoridad de certificación emite un certificado digital, lo hace por un periodo máximo de validez que oscila entre uno y cinco años (los certificados intermedios y raíz también la tienen, pero períodos más amplios). El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad o expiración viene indicada en el propio certificado digital. Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha expirado, de manera inesperada:

- El usuario del certificado cree que su clave privada o el token con el certificado se extravió o fue robado.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial, etc.

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Los principales mecanismos para verificar esto son las ***CRL (Certificate Revocation List)*** y ***OCSP (Online Certificate Status Protocol)***. Una CRL es una lista de certificados que la autoridad emisora decretó que ya no son válidos, y en los que no debe confiar ningún sistema de usuario. Un OCSP consulta ese listado y devuelve el estado de revocación de un certificado.
El vencimiento o revocación de un certificado ***no invalida todas*** las firmas realizadas con el mismo, sino tan solo aquellas que fueron realizadas en un momento posterior a su fecha y hora de caducidad/revocación.
En caso de necesitar revocar un certificado, deberá consultar a la Autoridad de Registro que se lo emitió. Adicionalmente puede consultar los procedimientos de revocación para Firma Token (con Clave Privada o PIN) y Firma Digital Remota.

Verificación

Existen muchas aplicaciones que permiten verificar la firma digital. En este instructivo se explica como hacerlo para documentos en formato PDF, mediante el software gratuito Xolido Sign (versión Desktop), y para Adobe Reader (válido para las versiones XI y DC). Debido a ciertas limitaciones del software de Adobe, ***recomendamos la utilización de Xolido***.
Condición previa, deberá haberse descargado e instalado el software elegido desde la página oficial.

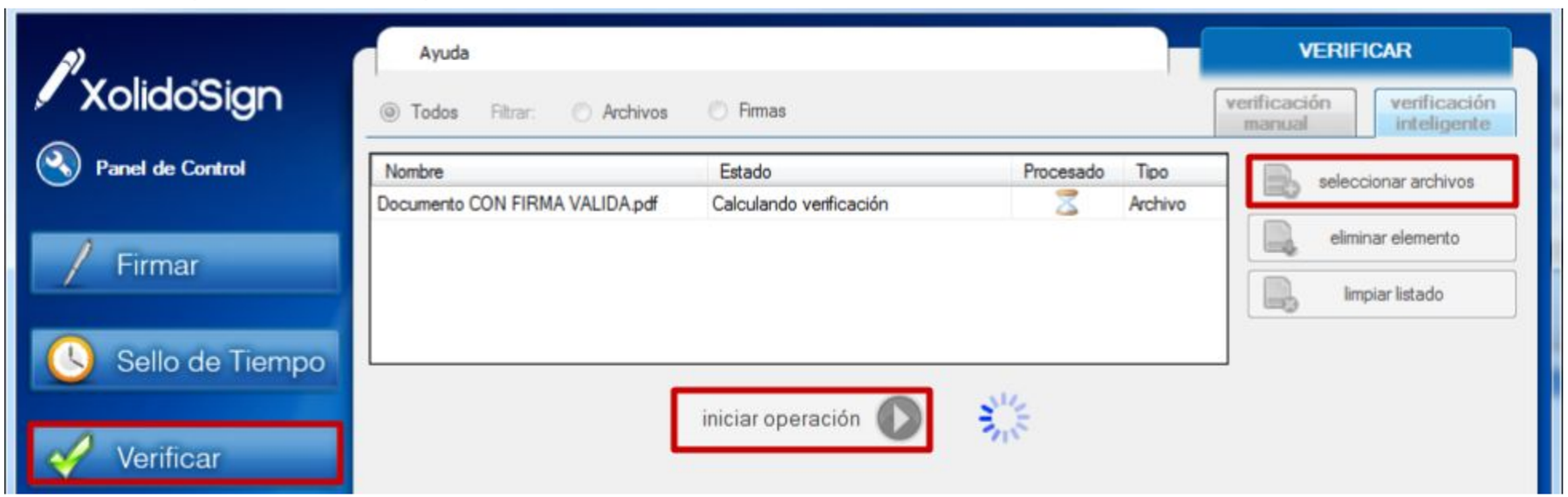
Importante: *Si la red donde se encuentra el equipo utiliza un servidor proxy o una configuración especial para acceder a Internet, deberá contactar a su administrador de red o asegurarse que el software elegido posee acceso. Esto permite al software realizar verificaciones sobre la hora de firma y estado de revocación del certificado.*

A. En el caso de Xólido, debe ingresar al menú Opciones Globales>Opciones Avanzadas>Configuración de Proxy, y seleccionar “usar configuración establecida en Internet Explorer” (los usuarios avanzados pueden optar por configurar manualmente el proxy)
B. En el caso de Adobe, la configuración por defecto utiliza la configuración de Internet Explorer. En caso de necesitar personalizarla, debe ingresar al menú Edición>Preferencias>Internet.

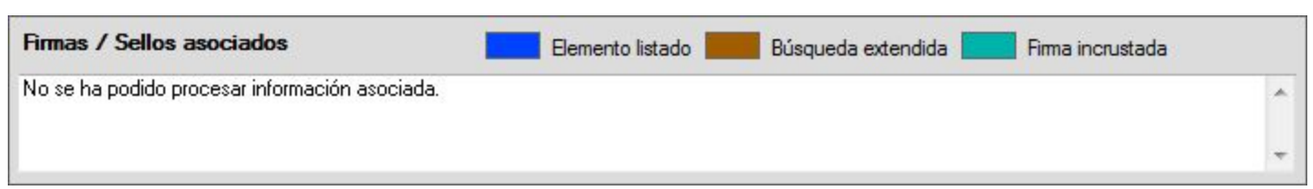
Xolido Sign

Xolido Sign es una aplicación especialmente diseñada para trabajar con firmas digitales. Sirve tanto para firmar como para verificar firmas en varios tipos de archivo. En este instructivo se detallará únicamente el procedimiento de verificación de firma en documentos PDF. Para mayor información, puede consultar en Manual de Usuario al que puede accederse desde la aplicación.

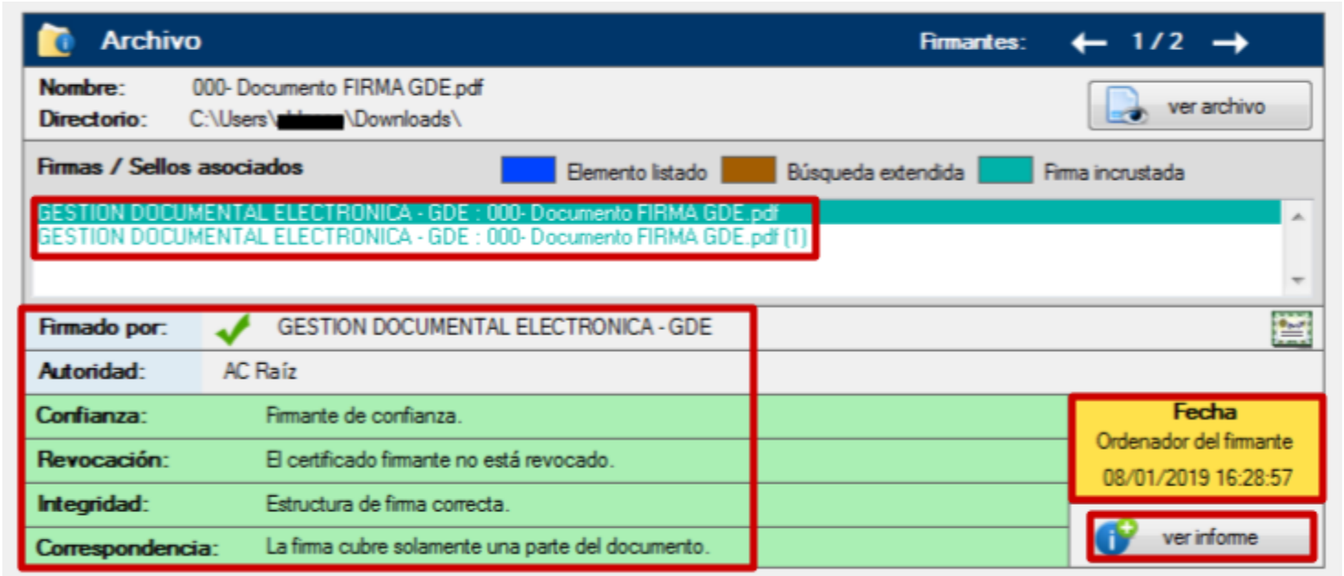
1. Abrir el programa e ingresar en la opción Verificar. Se utilizará la modalidad de “verificación inteligente” (opción por defecto).
2. Hacer click en “seleccionar archivos” y elegir el documento cuya firma desea verificar (verificar de a un documento por vez)
3. Finalmente, presionar “Iniciar operación”.



Si informa que “no ha podido procesar la información asociada”, ese archivo carece de firma digital.



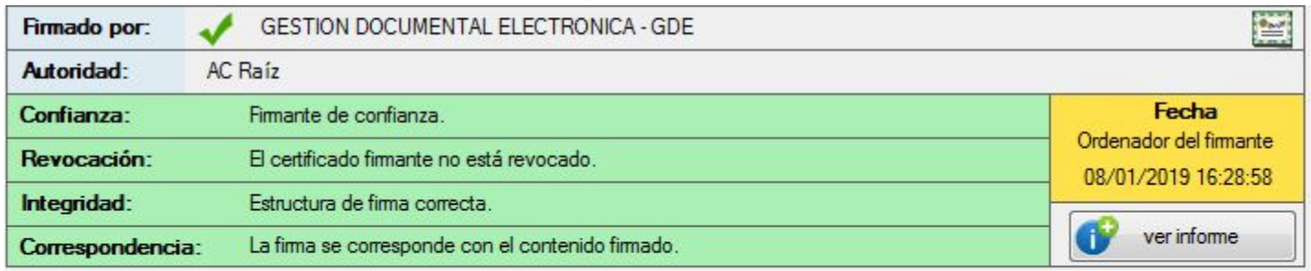
4. Una vez procesado el archivo, se abrirá un panel inferior que contiene toda la información de las firmas verificadas.
   También permite desplegar un análisis más detallado presionando el botón "***Ver informe***".



Firmas / Sellos asociados: Lista todas firmas que se hayan realizado sobre el documento. Las firmas deben seleccionarse una por una a fin de ver detalles y validez de cada una de ellas.
Firmado por: Indica el nombre del firmante de la firma seleccionada.
Autoridad: Indica qué autoridad emitió el certificado raíz (ver apartado Jerarquía de Certificados).
Confianza: Informa que el certificado empleado por el firmante es de confianza cuando se puede construir una cadena de confianza completa (los certificados intermedios y certificado raíz deben estar instalados).
Revocación: Verifica si el certificado de firma fue revocado por la autoridad certificante. Informa también si pudo comprobarse o no el estado de revocación.
Integridad: Informa si el proceso de firma se realizó correctamente.
Correspondencia: Informa si el documento coincide con el firmado, o fue modificado con posterioridad a la firma.
Momento de la Firma: Indica fecha y hora de la firma, así como de dónde procede este dato.

Respuestas Usuales

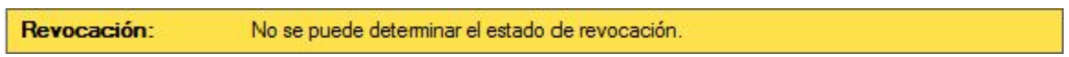
Idealmente, la verificación arrojará los siguientes resultados:



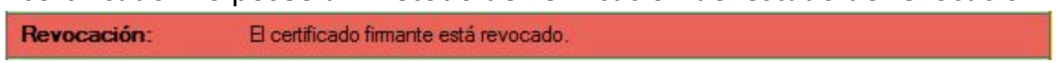
Esto indica que es una firma pasó satisfactoriamente todas las revisiones. Sin embargo también pueden obtenerse los siguientes resultados:

Este mensaje aparece cuando existen múltiples firmas en un documento. Cada firma añade un "anexo" al documento, y cada nueva firma se realiza sobre la anterior, por lo que solo la última de las firmas se realiza sobre el documento final completo.

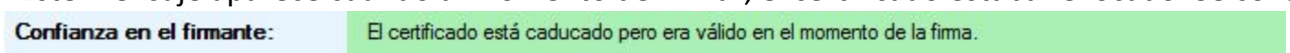
Todos los certificados de firma digital deben se emitidos por Certificadores Licenciados, y en consecuencia, como Autoridad siempre debe figurar "AC Raíz" o "AC Raíz de la República Argentina". Caso contrario, se considera *Firma Electrónica*.



El estado de revocación debería poder consultarse para cualquier certificado emitido por Autoridad Certificante. Este mensaje suele aparecer cuando el software no puede acceder a internet (ver apartado verificación) o cuando es *Firma Electrónica* y el certificador no posee un método de verificación del estado de revocación.



Este mensaje aparece cuando al momento de firmar, el certificado estaba revocado. Se considera *Firma Electrónica*.

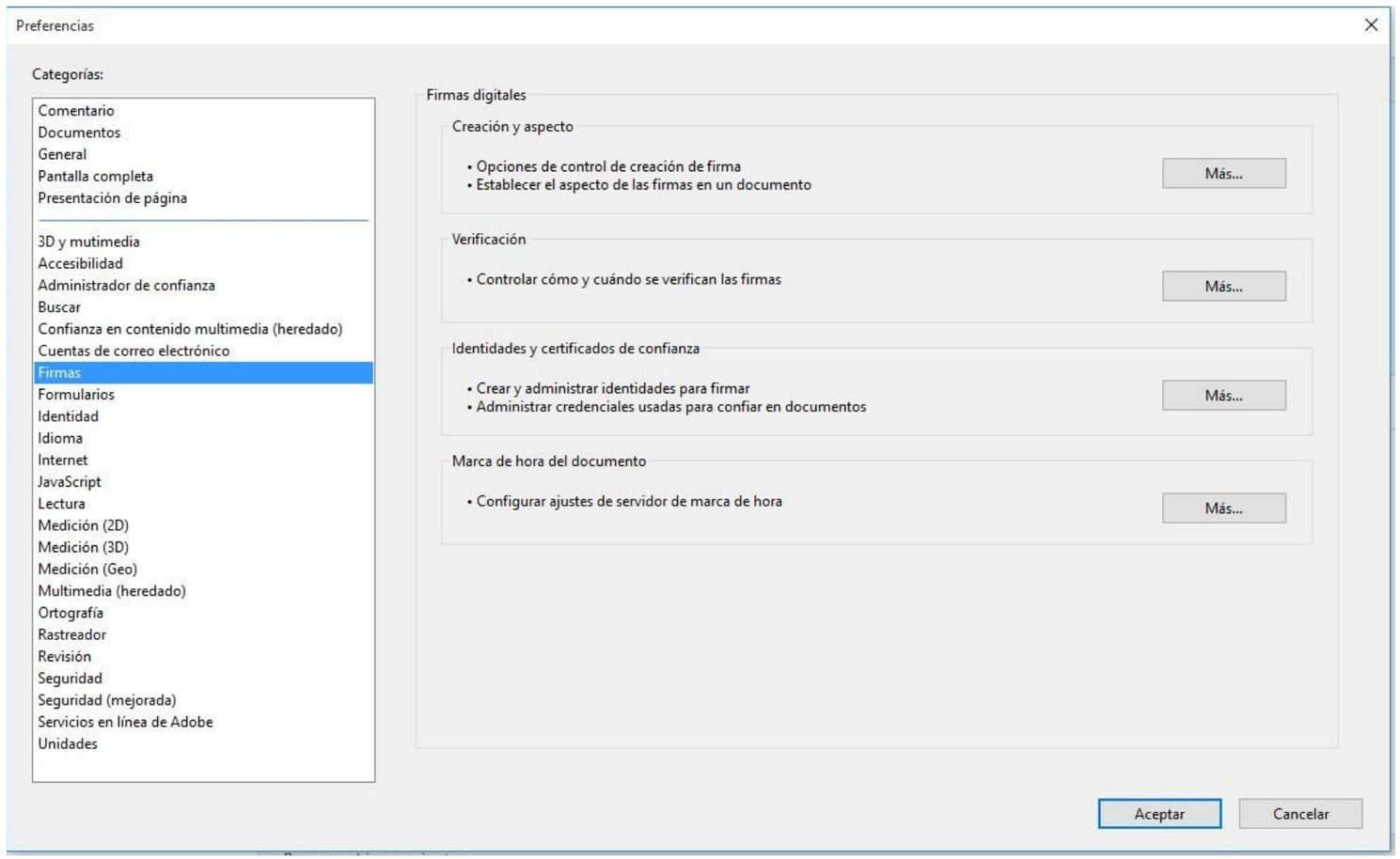


Cuando un certificado haya expirado o sido revocado, pero era válido al momento de la firma, la verificación inicial saldrá correcta. Ingresando al informe detallado, puede verse el estado actual de vigencia y revocación. Para asistencia sobre el informe detallado y otros mensajes de advertencia y error, consulte el manual de usuario de Xolido Sign.

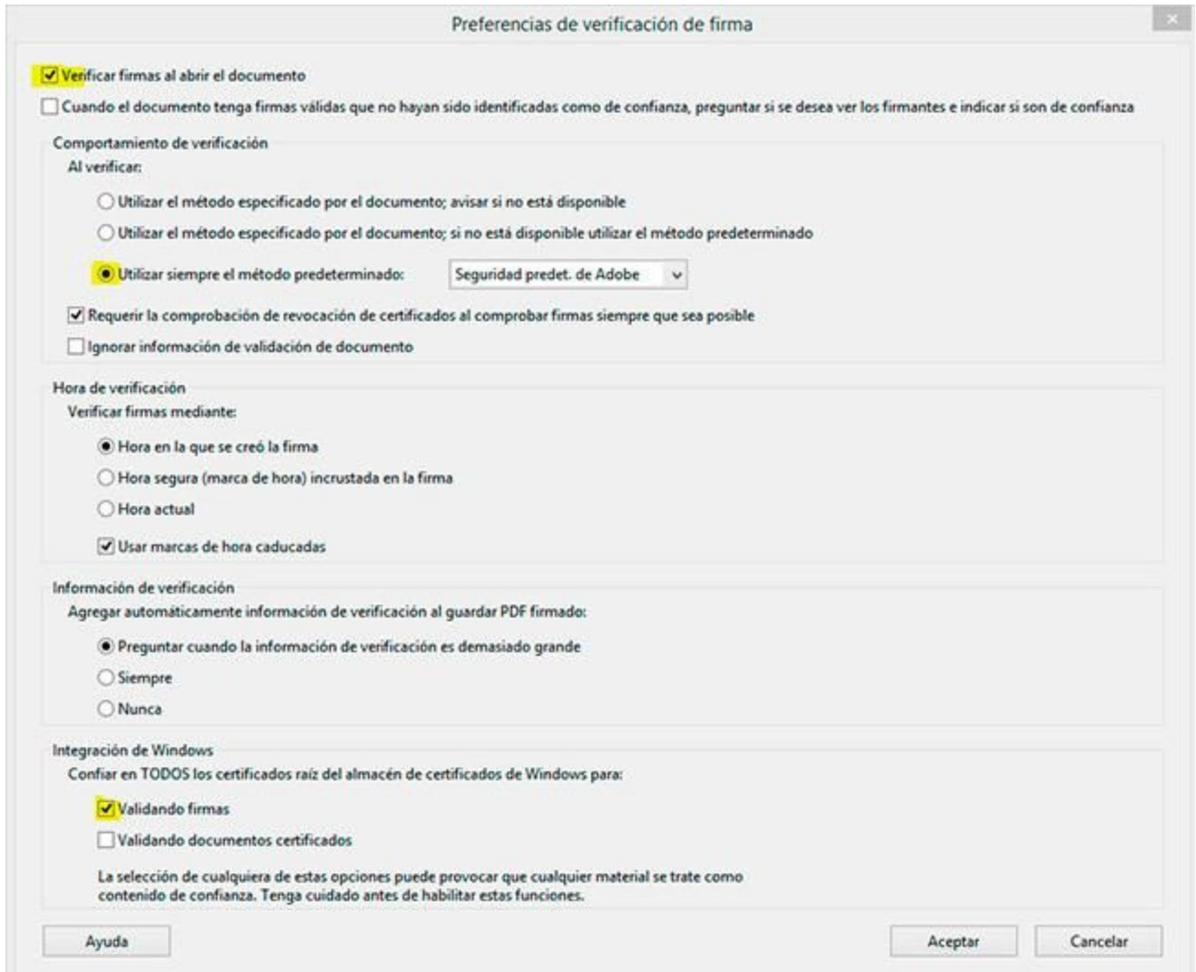
Adobe

Configuración

1. Ingresar al menú Edición > Preferencias, y allí, al apartado Firmas.
2. Desplegar las opciones de Verificación, presionando el botón Más.



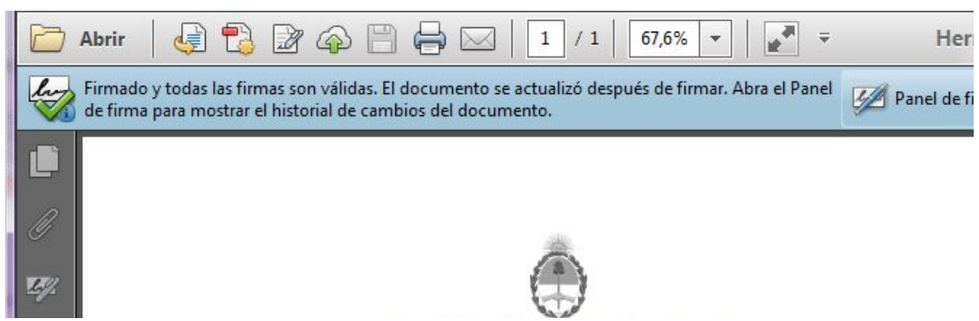
3. Tildar la opción “Verificar firmas al abrir el documento”.
4. En “Comportamiento de verificación”, seleccionar la opción “Utilizar siempre el método predeterminado, y allí, la opción “Seguridad predeterminada de Adobe”
5. En “Integración con Windows”, tildar la opción “Validando firmas”.



Verificación

1. Abrir el documento a validar mediante Adobe Reader.
    a. Si el documento fue descargado de la Web, y por defecto se abre con el visor del navegador Chrome, abrirlo desde el Explorador de Windows, o al descargar, presionar la flecha que se encuentra a la derecha del icono de documento descargado, y seleccionar la opción “Abrir con visor del sistema”.

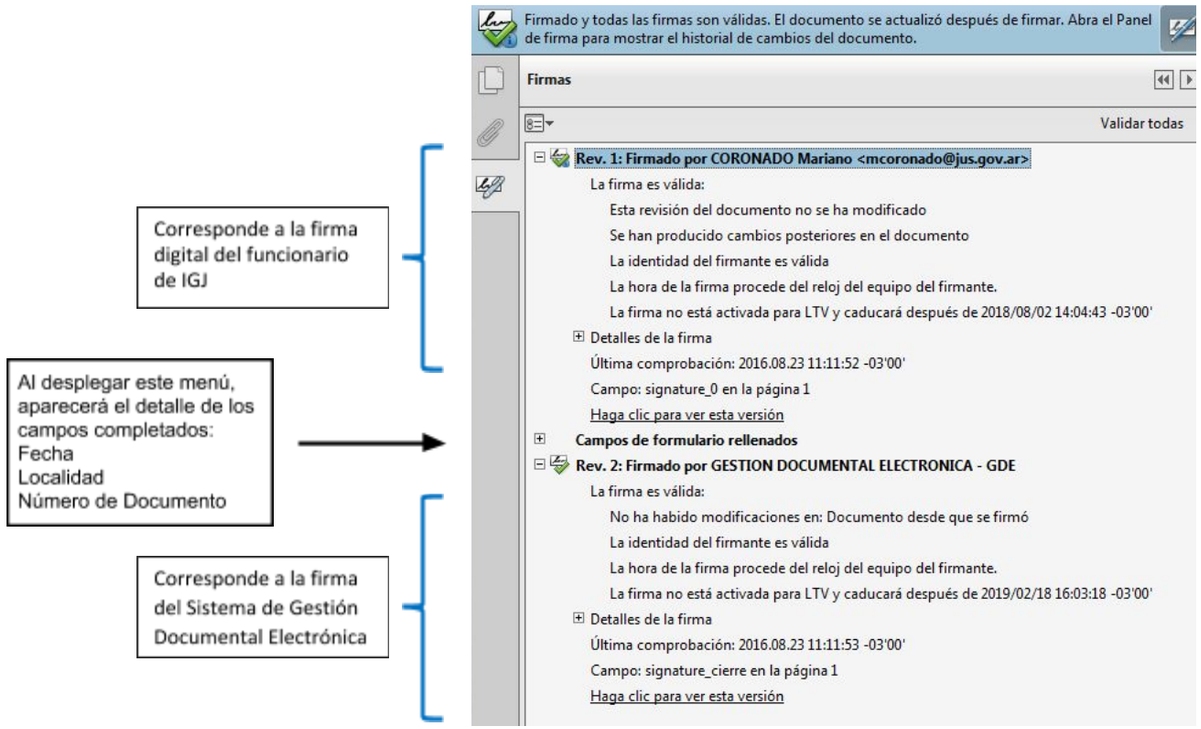
2. Al abrir el documento, en la parte superior, bajo la barra de herramientas, aparecerá el mensaje de comprobación de firmas.



Idealmente, aparecerá el mensaje en la imagen superior. La tilde verde indica que las firmas son válidas. El mensaje “El documento se actualizó después de firmar”, aparece siempre en los documentos firmados a través de las plataformas TAD/GDE (Trámites a Distancia - Gestión Documental Electrónica). Esto sucede porque luego de la firma del agente de la APN, el sistema incorpora el número de documento, fecha y localidad, y realiza una segunda firma para “sellar” el documento.
Puede abrir el panel de firma, presionando el icono correspondiente en la barra lateral izquierda, para comprobar datos adicionales de la firma.

Panel de Firma

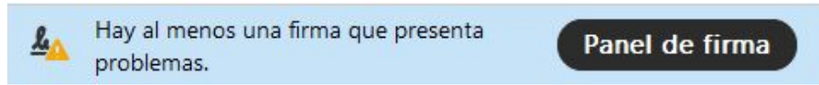
Este panel proporciona información acerca de la integridad, veracidad del documento firmado, así como información acerca del firmante, razón, fecha y hora de la firma.



Para conocer características adicionales del panel de firma, consulte el manual de adobe al respecto: https://helpx.adobe.com/es/acrobat/using/validating-digital-signatures.html

Otros Mensajes de Firma

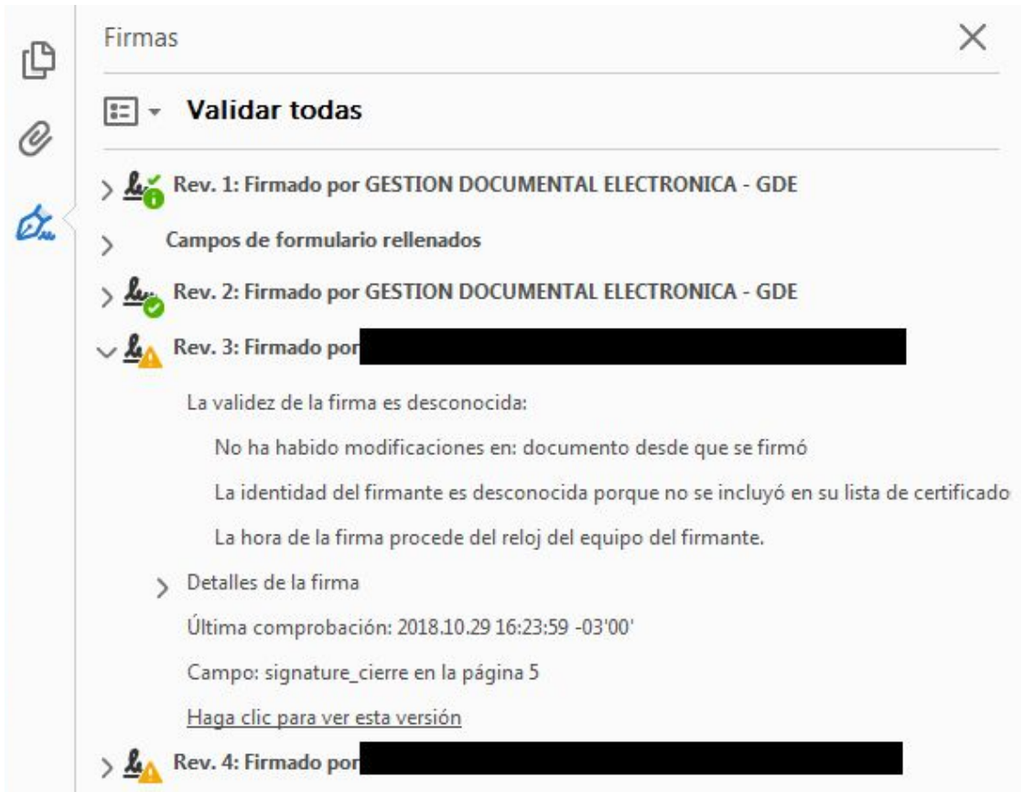
Si al abrir el documento, el panel superior de firmas no presenta la tilde verde que confirma la validez de la firma digital utilizada, hay que verificar los motivos.En caso que



aparezca:

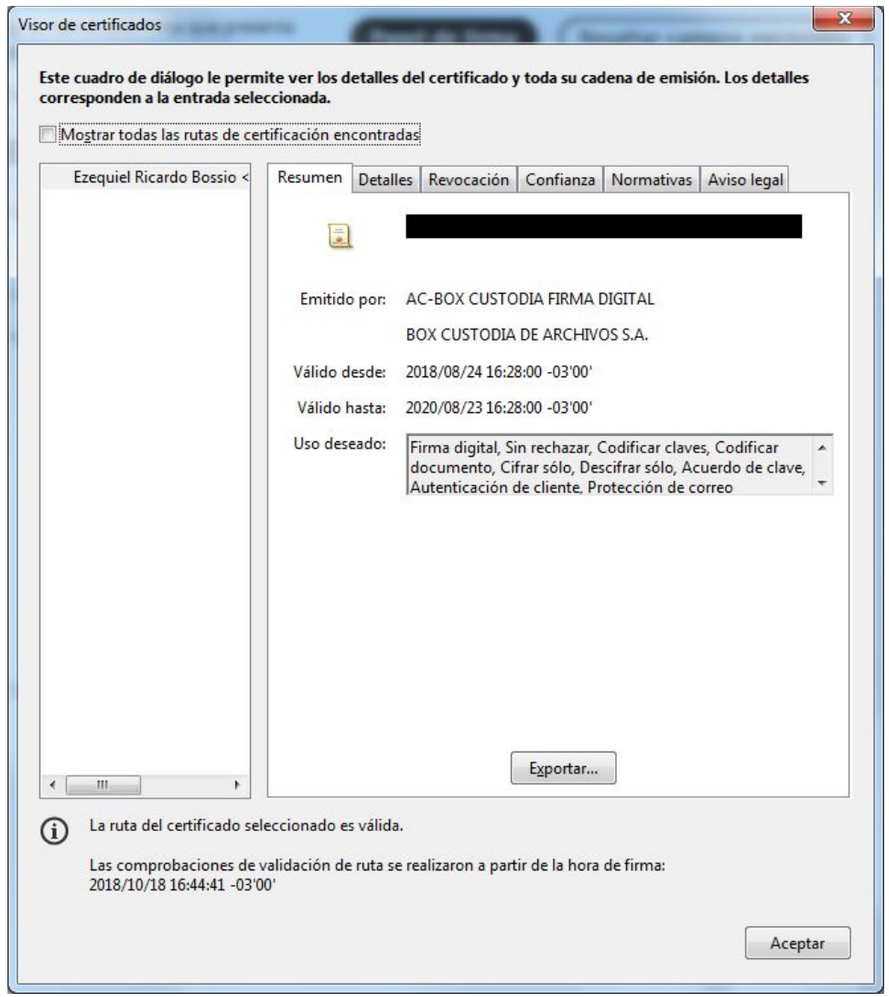
1. Desplegar el panel de firmas para ver los detalles de las mismas.

2. Allí, desplegar los datos de las firmas que presenten inconvenientes.
   Sí aparece el mensaje “La validez de la firma es desconocida” y debajo “La identidad del firmante es desconocida porque no se incluyó en su lista de certificados” esto puede deberse a:
   a. El Certificado Intermedio correspondiente a la Autoridad Certificante del firmante no fue correctamente instalado.
   b. La Autoridad Certificante no es un Certificador Licenciado. (es Firma Electrónica)
   c. El certificado fue generado por el mismo firmante. (es Firma Electrónica)



3. A fin de comprobar esto, desplegar la sección “Detalles de la firma, y allí, presionar “Detalles de Certificado”

Una ver abierto el Visor de certificados, deberá comprobar qué entidad aparece en el campo “Emitido por”, y verificar el listado completo de Certificadores Licenciados.
Si es un Certificador Licenciado (caso A), descargar el correspondiente certificado y realizar los pasos de la sección Instalación de Certificados AC.
En caso contrario, no se trata de una Firma Digital válida. Puede haber sido emitida por un certificador extranjero o local No Licenciado (caso B) o, si el emisor del certificado coincide con la identidad de la persona (tachada en la captura), de un certificado generado por el mismo firmante (caso C).



No Comprueba Revocación

En aquellos casos en que aparezca un problema con la firma, y al desplegar el panel un mensaje que indica:

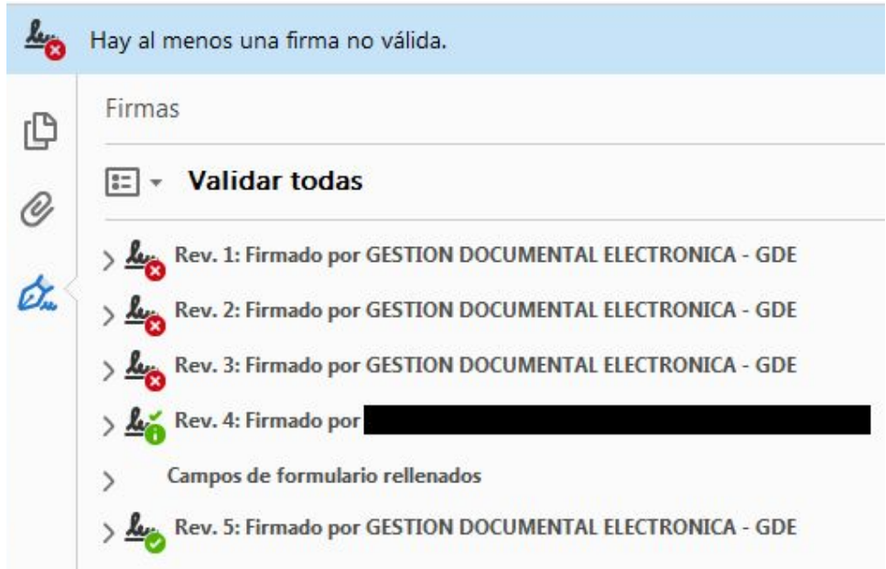
La firma es válida, pero no se ha podido comprobar la revocación de la identidad de los firmantes

deberán utilizar Xolido para validar la firma. Esto sucede generalmente con certificados vencidos, ya que Adobe no valida los mismos ni su estado de revocación cuando vencieron, por lo que no es posible determinar a simple vista si el certificado era válido al momento de la firma.

Firma Inválida

Una o más firmas del documento pueden presentar este problema. Los motivos para esto pueden ser varios, entre ellos:

- El documento fue modificado (fueron añadidas o quitadas páginas, se adjuntaron documentos, se modificó el texto o apariencia del documento en cualquier forma) luego de la firma.
- El documento fue firmado como versión final, luego de lo cual no permite añadir firmas ni ninguna otra operación sin invalidar las firmas anteriores.
- Ocurrió un error durante el proceso de firmado.



Al margen del motivo, no es posible corregir o reparar el documento que presenta este problema. El mismo se considera como carente de firma, digital o electrónica.

Sin Firma

Cuando el mensaje superior de firma no aparezca y tampoco exista el botón para desplegar el panel de firma, el documento PDF no está firmado. Es posible que se esté visualizando la versión del documento previa a la firma o por otros motivos la haya eliminado. Deberá rastrearse el documento correctamente firmado.

Para mayor detalle sobre las características de la Firma Digital en PDF, puede consultar el manual de Adobe (en inglés):
https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf

Links Útiles

- ***Ministerio de Producción - Firma Digital***
- ***Secretaría de Modernización Administrativa - Firma Digital***
- ***Plataforma de Firma Digital Remota (PFDR)***
  - ***Preguntas Frecuentes***
  - ***Normativa***
  - ***Firmador***
- ***Autoridad de Aplicación (AC-RAÍZ)***
- ***IGJ - Firma Digital***

Normativa

- Ley 25.506 - Ley de Firma Digital
- Decreto 2.628/2002 - Reglamentación de la Ley de Firma Digital
- Decreto 561/2016 - Sistema de Gestión Documental Electrónica
- Decreto 892/2017 - Autoridad Certificante MODERNIZACIÓN-PFDR (Plataforma de Firma Digital Remota)
- Resolución MM 399E/2016 - Políticas únicas de Licenciamiento y Certificación
- INFOLEG - Normativa Compilada sobre Firma Digital (apartado 1.4)