Firma Digital

Verificación de documentos firmados digitalmente
Anexos

Índice

Anexo I: Configuración de herramienta

Los pasos para verificar eficazmente un documento PDF firmado digitalmente son:

- Instalar el certificado raíz de la Autoridad Certificante - AC-RAÍZ y el certificado del Certificador Licenciado - AC-ONTI
- Configurar Acrobat Reader DC

Anexo I — Instalación de Certificados

(1) Ingresar con un explorador web a: https://www.argentina.gob.ar/valida-los-documentos-electronicos-firmados-digitalmente-0

(2) Una vez en el sitio, descargar el instalador de los certificados haciendo click en el link "cadena de certificados":

¿Cómo hago?

Instalar los certificados por única vez.

Deberás instalar los certificados para poder comprobar la autoría del firmante:

Instalador para Windows:

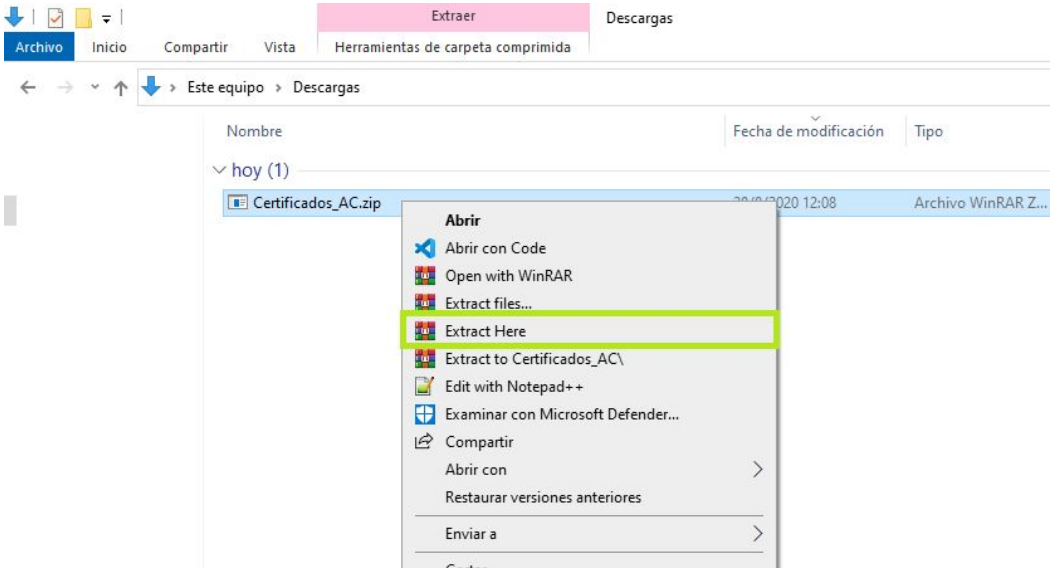
- Incorporá la cadena de certificados emitidos por AC-Raíz, incluye todos los certificados de las autoridades certificantes públicas y privadas.

Descarga manual de certificados para cualquier sistema operativo:

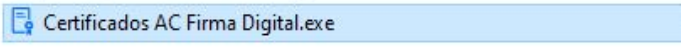
- Certificado de la AC Raíz de la República Argentina 2007
- Certificado de la AC Raíz de la República Argentina 2016
- NUEVO Certificado de la AC ONTI 2020
- Certificado de la AC ONTI
- Certificado de la AC MODERNIZACIÓN-PFDR

(3) Luego realizar los siguientes pasos con **el archivo** descargado:

(3.A) **Extraer el contenido del archivo:** haciendo click derecho sobre el mismo, y seleccionando la opción "*Extraer Aqui*" o "*Extract Here*"

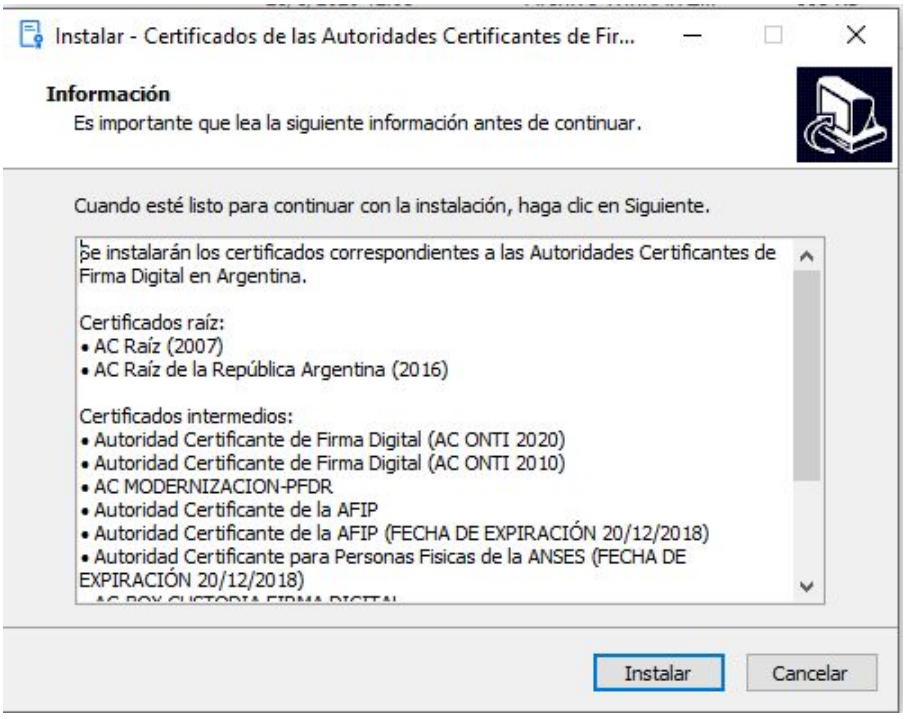


Haciendo esto se descomprime el archivo "**Certificados AC Firma Digital.exe**"



(3.B) Ejecute el archivo extraido, llamado "**Certificados AC Firma Digital.exe**" haciendo doble click sobre el mismo.

(3.C) En la nueva ventana haga click sobre el botón "**Instalar**".



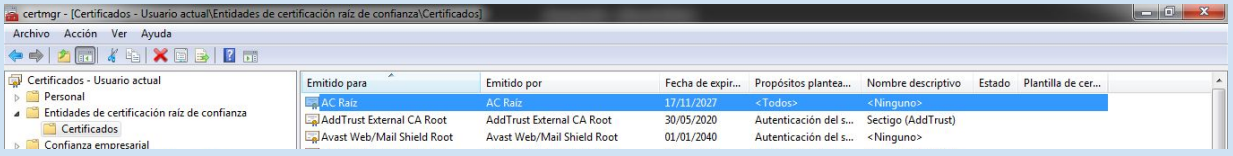
(4) Una vez descargado e instalados los certificados en el Sistema Operativo, se procederá a configurar Acrobat Reader DC.

(5) Si se desea, puede **verificar** que los certificados están correctamente instalados. Para ello:

Desde el menú de inicio de Windows, ir a:
Panel de Control >>
Administrador de credenciales >>
Agregar una credencial basada en certificado >>
Abrir el administrador de certificados.

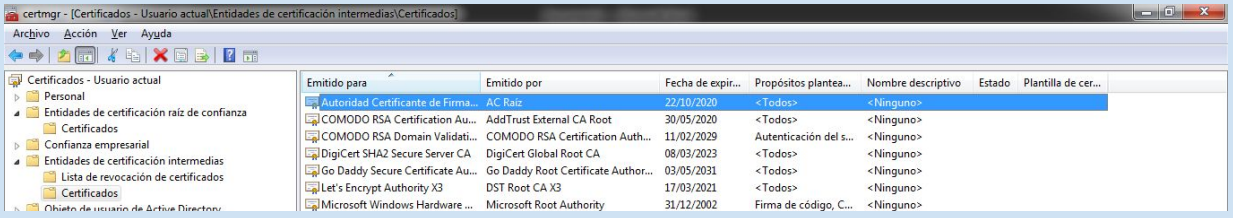
Localizar la entrada:
Entidades de certificación de raíz de confianza >> Certificados

Debe figurar: **AC Raíz - AC Raiz**



Localizar la entrada:
Entidades de certificación intermedias >> Certificados

Debe figurar: **Autoridad Certificante de Firma Digital - AC Raíz**



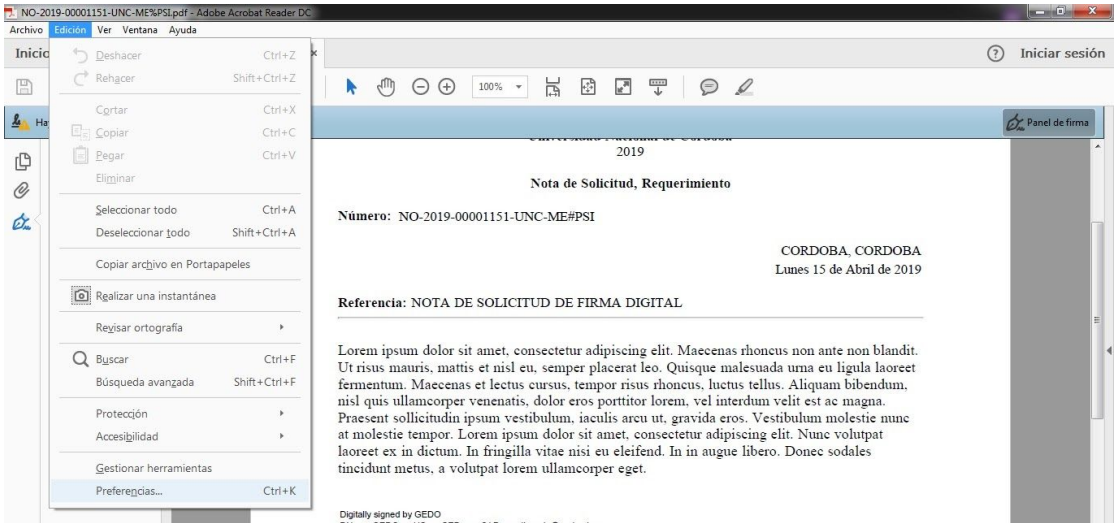
(6) Si tiene en su PC la configuración aquí indicada, prosiga con la configuración de Acrobat Reader. Caso contrario, revise los pasos anteriores.

Anexo I — Configuración de Acrobat DC

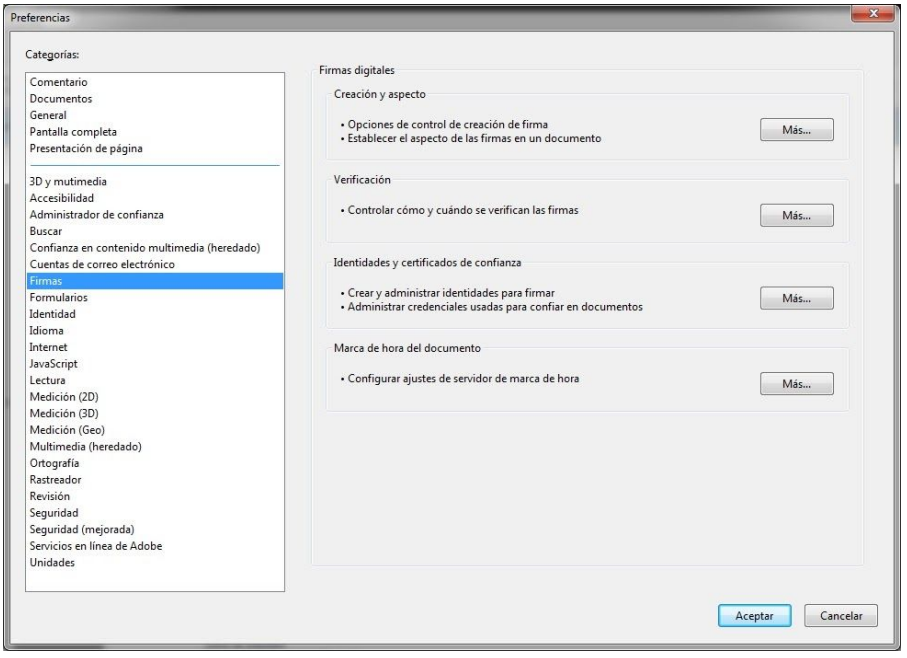
La configuración de Acrobat Reader DC presenta dos pasos:

Anexo I — Configuración de Acrobat DC — Paso I

(1) Ingresar a Acrobat Reader DC e ir al menú Edición >> Preferencias



(2) Localizar la categoría **Firmas**, sección **Verificación**. Hacer clic en el botón **Más...**



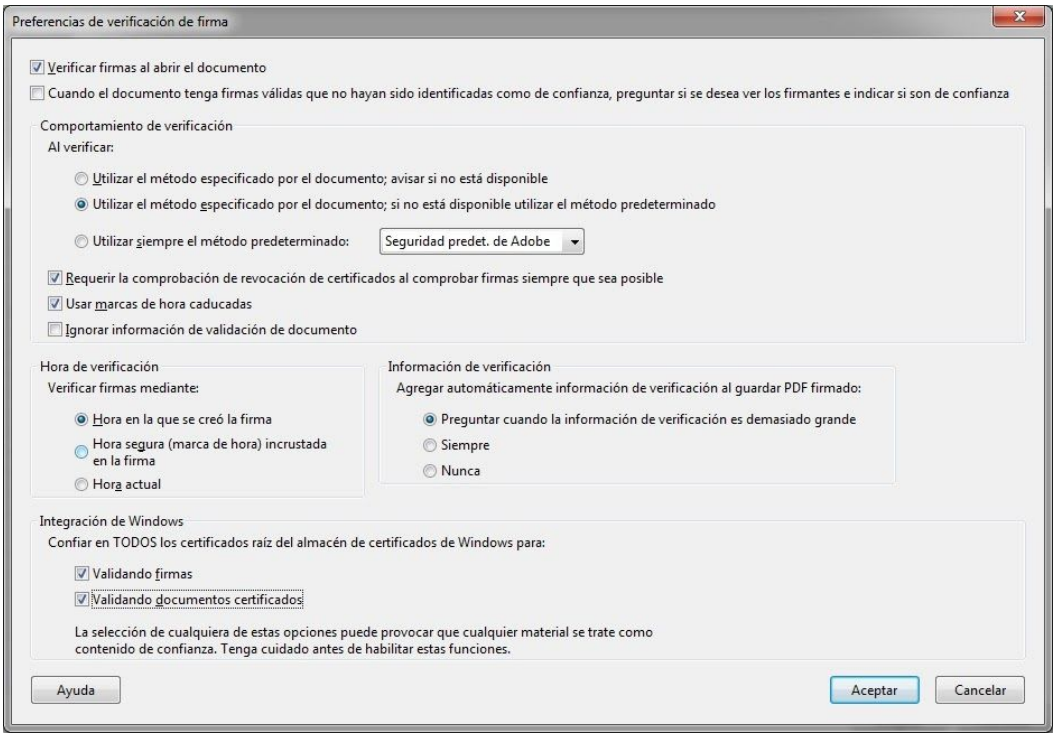
(3) Ahora dentro de la ventana "*Preferencias de verificación de firma*":

(3.A) Tildar la opción *"Verificar firmas al abrir el documento"*.

(3.B) En la sección *"Comportamiento de verificación"*:
- ✓ Seleccionar la opción *"Utilizar siempre el método predeterminado"*, y alli, la opcion *"Seguridad predeterminada de Adobe"*

(3.C) En la sección *"Integración de Windows"*, tildar ambas opciones:
- ✓ *Validando Firmas*
- ✓ *Validando documentos certificados*

(3.D) Por último hacer clic en el botón Aceptar.



(4) Abrir un documento GDE con Acrobat Reader.

Anexo II:
Herramienta de Software Xolido Sign

Esta herramienta para la validación de firmas digitales puede descargarse desde - https://www.xolido.com/lang/xolidosign/ - con una licencia de uso gratuito que será suficiente.

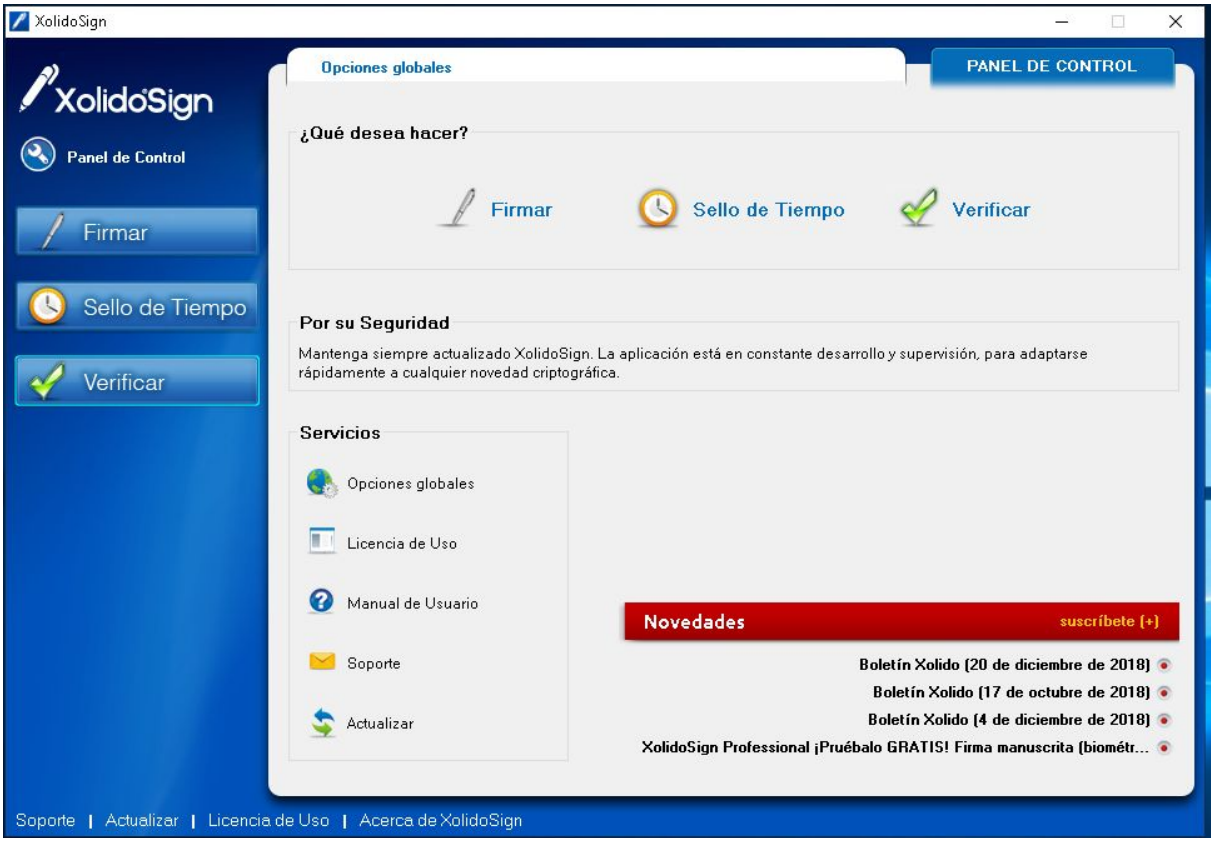
Para el caso mencionado en el apartado de Verificación de firmas, en donde figura el siguiente mensaje en el Software de **Acrobat**.

Y en el Panel de Firma figura 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 certificado".

Deberíamos proceder a instalar y ejecutar el software **Xolido Sign.** Una vez instalado el mismo lo ejecutamos y seguimos los pasos mostrados a continuación

(1) Una vez dentro del mismo Seleccionamos la opción "*Verificar*"



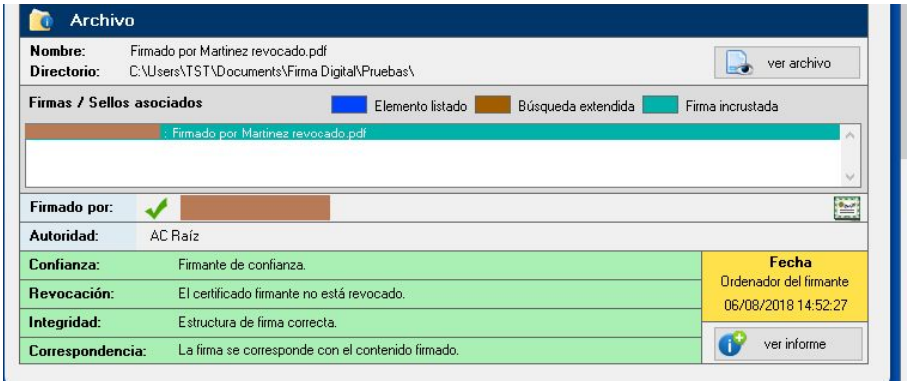
(2) Acceder a la pestaña "***Verificación inteligente***". Dentro de esta ventana vaya a la opción "***seleccionar archivos***"

(5.A) Busque el **archivo** cuya firma digital desea validar.
(5.B) Una vez seleccionado el archivo, haga clic en la opción "***iniciar operación***".

---

(3) Aquí debemos fijarnos en la parte inferior de la ventana (la sección "***Archivo***"). En la sección "***Firmas/Sellos asociados***" podemos seleccionar las distintas firmas incrustadas en el documento. y ver la información que le corresponde:

(5.A) Firmado por: indica quien es el Firmante de la firma seleccionada, sea una persona o entidad.
(5.B) Autoridad: Indica que autoridad emitió el certificado. deberían ser siempre emitidos por certificadores licenciados y debería figurar en nuestro caso "AC Raíz" o "Autoridad Certificante de Firma Digital"
(5.C) Confianza: La aplicación establece si el certificado empleado es de confianza, cuando se puede construir una cadena de confianza completa y el certificado raíz de esta se encuentra instalado en el almacén de entidades de confianza de Windows.
(5.D) Revocación: Verifica si el certificado de la firma fue revocado por la autoridad certificante.
(5.E) Integridad: Informa si el proceso de validación de firma se pudo realizar correctamente.
(5.F) Correspondencia: Informa si el documento coincide con el firmado, o fue modificado con posterioridad a la firma.



(4) En caso de que los resultados figuren como se muestra en la pantalla anterior, esto significa que la verificación inicial resultó correcta. Ahora puede verificar el detalle del estado de revocación.

---

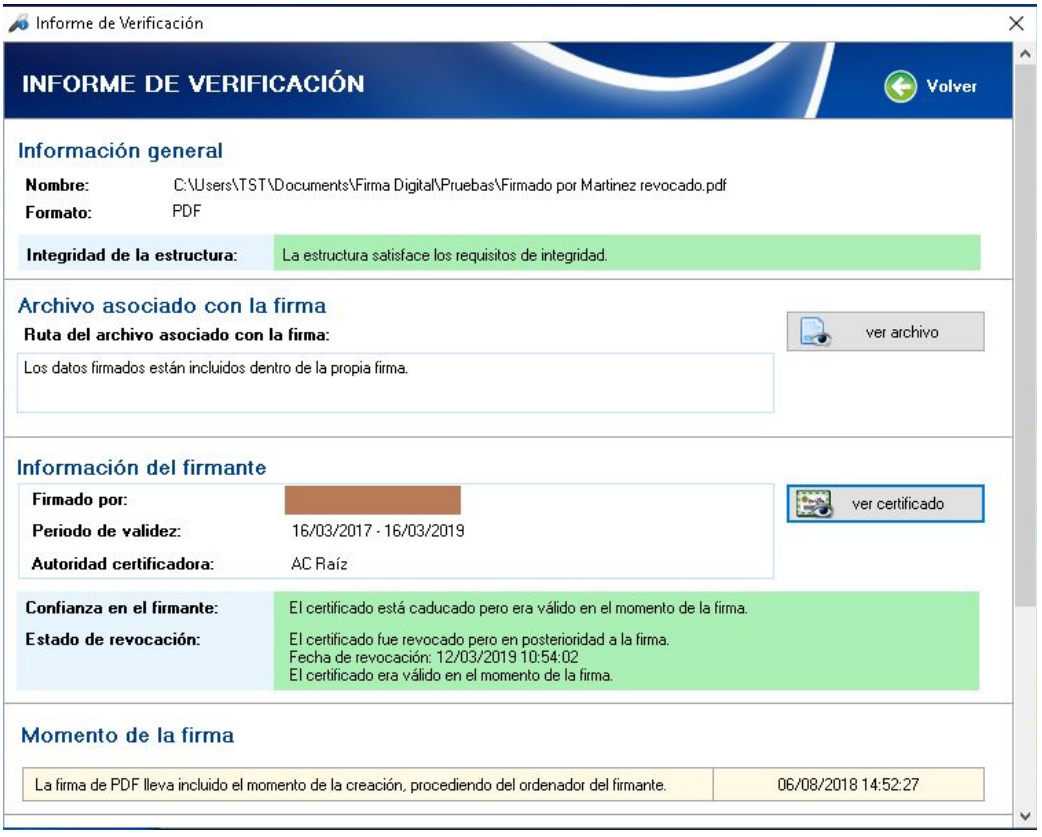
(5) Al ingresar a la opción "*Ver informe*" (para visualizar el informe detallado) llegaríamos a la siguiente pantalla en donde:

(5.A) En la sección "**Información del Firmante**" y en el *Ítem* "**confianza en el firmante**" deberia aparecer el mensaje:

"El certificado está caducado pero era válido en el momento de la firma"

Esto indica que el certificado fue revocado por la autoridad certificante, en la fecha indicada como fecha final del periodo de validez, pero que en el momento en que el documento fue firmado, la firma era válida.

Por lo tanto la firma contenida dentro del documento se considera válida, y se sigue considerando Firma Digital.



Anexo III: Herramienta Adobe Acrobat Pro 9.X.X

Para el caso de la herramienta **Acrobat Pro (version 9.X.X)**, la funcionalidad en cuanto a la validación de firmas digitales es idéntica a la de **Acrobat Reader (versiones DC y XI)**, a excepción de cómo son tratadas las modificaciones que se consideran comentarios.

Comentarios hechos y vistos desde Acrobat Pro

Cuando se escribe una anotación o comentario desde Acrobat Pro en un archivo firmado digitalmente, este programa no lo detecta como una modificación al archivo ya que los reconoce como comentarios y puede manejarlos como contenido separado del archivo original.

Ante el agregado de cualquier comentario o anotación considerado como válido por Acrobat Pro, la firma seguirá figurando como válida, (suponiendo que figuraba de esta manera previo a agregar el comentario).

Cómo leer el archivo sin comentarios.

Si posee un documento pdf, firmado digitalmente y desde el software **Acrobat Pro** la firma figura como válida, para poder leer el documento con la **seguridad** de que no hay ningún comentario sobre el mismo que pudiera causar confusión, entonces:

- Dentro del software con el documento abierto, seleccionar la opción ***"Comments > Comment View > Hide All Comments".*** Tras hacer esto, todas las anotaciones y comentarios estarán ocultos y entonces se podrá visualizar el archivo sin ningún tipo de comentario o anotación.
- Para revertir esto en caso de que necesite visualizar los comentarios hechos sobre el archivo, seleccionar la opción ***"Comments > Comment View > Hide All Comments".***

Anexo IV: Archivos Embebidos y Combinados

Archivo firmado digitalmente, con adjuntos no firmados

Si un archivo está firmado digitalmente **no es posible agregar, eliminar ni modificar** sus archivos adjuntos sin invalidar la firma (del *archivo contenedor*), ya que, todos los archivos adjuntos se consideran **contenido firmado**.

Por lo tanto, mientras el archivo adjunto no se guarde por separado (*Guardar como copia*), el mismo se considera **firmado digitalmente** por la misma firma del *archivo contenedor*. Todos los archivos adjuntos tienen que ser agregados antes de la primera firma para no invalidarla.

Archivo firmado digitalmente, con adjuntos firmados

En el caso de que un archivo firmado digitalmente tenga adjuntos, archivos que estaban firmados digitalmente previo a ser adjuntados al archivo contenedor:

- Si un archivo adjunto es **eliminado** del archivo contenedor, entonces la firma del archivo contenedor pasará a ser **invalida**,.
- Si un archivo adjunto es **modificado**, entonces tanto la firma del archivo contenedor como la firma del archivo adjunto modificado pasarán a ser **inválidas**.

Combinación de Archivos Firmados Digitalmente

En caso de utilizar una herramienta como **IL PDF**, **Acrobat Pro** o **Acrobat Pro DC**, para combinar archivos pdf. Si estos archivos están firmados digitalmente, las firmas de ambos archivos se verán eliminadas/removidas del nuevo archivo que será generado. Esto sucede ya que estas herramientas al combinar archivos pdf, en realidad están creando un nuevo archivo.
En este caso se deberá volver a firmar el archivo generado para que pueda ser considerado firmado digitalmente..

Portfolios de PDF

Algunas herramientas avanzadas como **Acrobat Pro DC** y **Acrobat Pro 9.X.X**, permiten la creación de lo que se llama portfolio de PDF.

El portfolio como tal no puede ser firmado digitalmente, pero los archivos dentro del mismos si.

Si un archivo se encuentra firmado digitalmente, esta firma solo sirve para validar la integridad y confiabilidad de dicho archivo. Firmar, actualizar o modificar un archivo no afecta las firmas de los otros archivos.

Anexo V: Marco Teórico

¿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

Cualquier 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 Nº 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-RAIZ**), 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 **P**lataforma de **F**irma **D**igital **R**emota (**PFDR**) .

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:

1º - Autoridad Certificante Raíz - AC-RAIZ

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-RAÍZ RA 2007 (necesario para validar Firmas Digitales Token)

- Certificado AC-RAÍZ RA V2 (necesario para validar Firmas Digitales Cloud)

Los cuales pueden descargarse manualmente de la página:
https://www.argentina.gob.ar/modernizacion/administrativa/firmadigital/acraiz

2º - 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 documentos firmados por personas que hayan adquirido su firma digital se presenta a continuación el enlace con el listado completo de Certificadores Licenciados:

https://www.argentina.gob.ar/firmadigital/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.

Esto permitirá validar los documentos firmados con certificados provistos por ese emisor, aunque 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 .

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 por 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, cambio de autoridad de una Unidad Académica

- 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 este 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 .

Aplicaciones de 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 **Adobe Reader** (válido para las versiones **XI** y **DC**).

Adicionalmente, y debido a ciertas limitaciones del software de Adobe, en el Anexo II de este manual, se explica cómo validar ciertos casos específicos con la software gratuito **Xolido Sign**.

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.