Secretaría de
MODERNIZACIÓN DEL ESTADO, CIENCIA Y TECNOLOGÍA
Secretaría General de la Gobernación
Gobierno de Entre Ríos

Firma Digital

Manual de Procedimientos - Verificar documentos firmados digitalmente

Secretaría de Modernización de Estado, Ciencia y Tecnología – Entre Ríos
Autoridad de Registro

¿Qué es la firma digital?

La firma digital es una herramienta tecnológica que permite garantizar la autenticidad, integridad, exclusividad, no repudio y validez de los documentos digitales posibilitando que éstos posean la misma característica que los documentos firmados mediante firma hológrafa (de puño y letra), exclusiva de los documentos en papel. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
Cada titular de una firma digital posee un par de claves asociadas, una privada y otra pública, generada mediante un proceso matemático.
La **CLAVE PRIVADA** es utilizada por su titular para firmar digitalmente un documento o mensaje, es secreta y mantenida por ese titular bajo su exclusiva responsabilidad.
La **CLAVE PÚBLICA** es utilizada por el receptor de un documento o mensaje firmado para verificar la integridad y la autenticidad, asegurando el "no repudio".
Ambas claves se encuentran asociadas entre sí por las características especiales del proceso matemático.
Según la legislación argentina, si un documento firmado digitalmente es verificado correctamente, se presume, salvo prueba en contrario, que proviene del suscriptor del certificado asociado y que no fue modificado.

¿Qué son los certificados digitales?

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado.
En su forma más simple, el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo.

Los Certificados con nivel de seguridad por Software tienen la ventaja de no necesitar ningún hardware especial, sin costos, posibilitando su uso masivo. Solo requiere instalar el certificado en la PC que se utilizará para firmar digitalmente documentos. El sistema solicitará el ingreso de la clave privada para firmar documentos.
Por su parte los Certificados con nivel de seguridad por Hardware brindan una mayor seguridad ya que los datos privados del titular son almacenados en un dispositivo criptográfico especial (TOKEN). Para firmar digitalmente, el sistema solicitará que se conecte el dispositivo criptográfico y se ingrese la clave privada.

Terceros Usuarios:

Son Terceros Usuarios de los certificados emitidos bajo la Política Única de Certificación, toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo al Anexo I del Decreto N° 2628/2002.

Verificar firmas digitales

Aunque existen diferentes procedimientos y programas para firmar y verificar la validez de la firma digital, se ha desarrollado una plataforma específica para realizar dichos procedimientos. **XolidoSign (Xolido Systems S.A.)**, es un programa gratuito que permite firmar, verificar y sellar con tiempo documentos electrónicamente en tu computadora (https://www.xolido.com/lang/xolidosign/xolidosigndesktop/). Esta aplicación está disponible para plataformas Windows proporcionada por Xolido Systems. 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, etc. XolidoSign 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 documentos digitales, desde estudiantes, ingenieros, profesionales de cualquier índole, PYMES, autónomos, funcionarios, etc.
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). Trabaja tanto con certificados que tengamos instalados en nuestros equipos como con también tarjetas criptográficas (token).

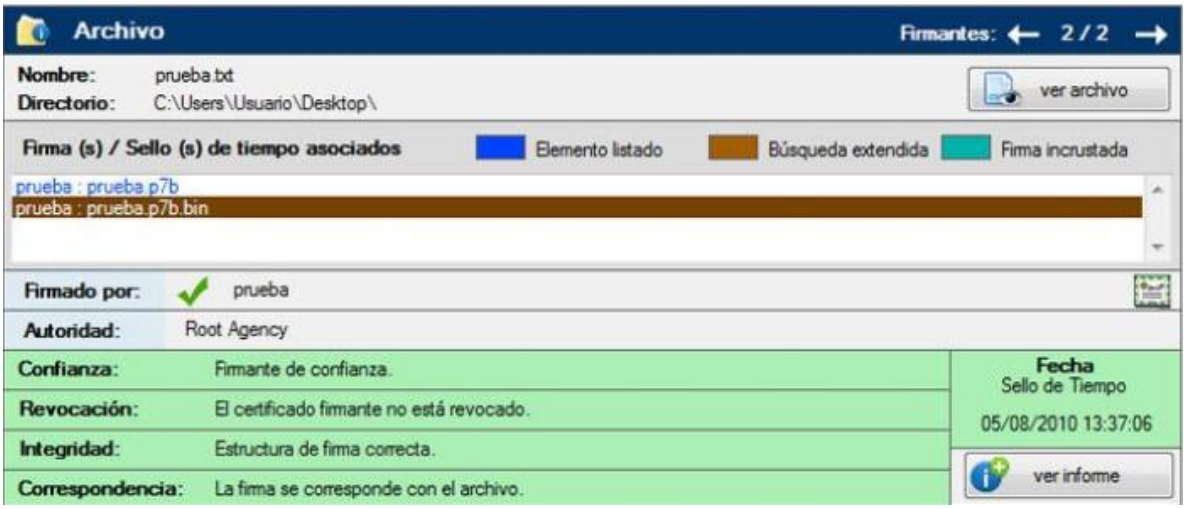
Verificar Firma Digital con XolidoSign

Podemos verificar documentos que fueron firmados por terceros y chequear veracidad, para esto presionamos en el botón "Verificar" del panel izquierdo o del panel principal. Cuenta con dos funcionalidades para verificar documentos, "Verificación Manual" y "Verificación Inteligente".
El modo de **verificación inteligente** realiza un proceso automático de emparejamientos y asociaciones entre los archivos y las firmas incluidas en la lista de selección y proporciona el estado de validez de firmas, sellos y archivos.

Además el sistema trata de encontrar firmas asociadas 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.

El modo de **verificación manual** se emplea cuando el usuario desea contrastar una serie de firmas 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.

Se debe seleccionar el o los archivos a verificar (otra opción es arrastrarlos hasta la ventana principal). Presionamos el botón **"Iniciar Operación"** para dar curso a la verificación.
* También se puede agregar o eliminar archivos de la lista, como así también limpiar todo el listado presionando en los botones correspondientes del menú ubicado a la derecha.
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. Cuando el elemento se procesa como archivo, aparecerá el resumen que se muestra en la imagen a continuación.



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.
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.

Presenta la posibilidad de ver un informe más detallado, presionando el botón "**ver informe**" en la posición inferior derecha. 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.
En este caso, la pantalla que muestra el programa se divide en cinco partes:
Información General
Muestra información del archivo firmado, como ser la ruta de acceso, el formato, integridad, etc.
Archivo asociado a la firma
Muestra información del archivo asociado a la firma (si existe) o si esta incrustada dentro del mismo.

Información del firmante
Muestra información del firmante, como su nombre, la autoridad certificante, la validez de su certificado, etc.
Momento de la firma.
Muestra detalles del momento que se realizó la firma.
Correspondencia de la firma con el archivo asociado
Muestra información del encriptado y des encriptado, como ser el algoritmo utilizado, el código, etc.