¿Qué es la firma digital?
Es la firma que permite saber que un documento digital corresponde a una persona determinada. Una serie de operaciones matemáticas hacen que esa firma sea única, auténtica y pueda ser verificada por la persona que recibe el documento.
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.

¿Cuales son los requisitos legales de la firma?
Los requisito que cumplimentan son :

- Autenticidad: Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- Integridad: Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- Exclusividad: Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- No repudio: Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.
- Validez: Haber sido producida con un certificado emitido por un Certificador Licenciado.

¿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

¿Como es la arquitectura de firma?
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.

¿Como es el proceso de 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.

¿Qué son los documentos digitales?
Los documentos digitales son, por ejemplo, texto escrito en un procesador de textos, un email, un sitio web, una planilla de cálculo y toda información contenida en un soporte electrónico.

¿La firma digital cumple la misma función que la firma de puño y letra?
Sí. Cuando por ley es obligatorio que un documento lleve firma, esa obligación se puede cumplir con la firma digital.

¿Cual es el marco que valida Firma Digital?

La validez se basa en 4 puntos :

- Autenticidad: Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- Integridad: Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- Exclusividad: Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- No repudio: Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.

¿Qué archivos se puede firmar?

Se pueden firmar infinidades de extensiones, las principales y la que los software tradicional trabajan son:

- Datos enviados a través de un formulario web.
- Una imagen, fotos o música.
- Un base de datos.
- Un disco rígido, un CD o un DVD.
- Una página o un sitio de Internet.
- Una transacción electrónica o un e-mail.
- Una hoja de cálculo o un documento de texto.
- El código fuente de un programa o un software.
- Uno o varios archivos en general (lote)

¿Por qué firmar un PDF?

Desde su versión 1.5, el formato PDF soporta la incorporación de firmas digitales incrustadas. Estas firmas están formateadas en el documento de acuerdo con el estándar PKCS#7.

¿Que es criptografía?

La palabra criptografía viene del griego, kryptos (escondido) y graphein (escribir).Podemos definir en el ámbito de Firma Digital que la Criptografía como una técnica o conglomerado de técnicas, tendientes a la protéger texto original a través del cifrado que prueba la integridad

¿Que no es firmar digital?

Los siguientes ejemplos son errores de interpretar que existe firma digital cuando:

- Una firma digitalizada (una firma manuscrita escaneada).
- Una contraseña o password para validar
- Un sistema biométrico donde se registre la huella
- Un sistema de autenticación: este requisito sólo no alcanza.
- Una firma electrónica, este requiere
- Un documento encriptado (solo se garantiza la confidencialidad).

¿Qué son los certificados?

Los certificados de clave pública son documentos digitales firmados digitalmente por una Autoridad Certificante que vinculan la clave pública de una persona a sus datos de identidad

¿Cuando debo instalar los 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. **Importante :** Para instalar el certificado AC se recomienda haber iniciado una sesión con un usuario con permisos de administrador en su PC, seguir los siguientes paso :

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 indicándose

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

¿Cómo puedo reconocer si un documento está firmado digitalmente?

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.

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 superior a XI y DC).
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 a internet. 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

Para verificar el hash en Xolido Sign se puede realizar 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”.

Para verificar el hash en Adobe se puede realizar desde la aplicación donde muestra el panel Firmas muestra sobre cada firma digital en el documento actual y el historial de cambios del documento desde la primera firma digital. Cada firma digital tiene un icono que identifica su estado de verificación. Los detalles de verificación se muestran debajo de cada firma. Para verlos, expanda la firma correspondiente. El panel Firmas también proporciona información sobre la hora en que se firmó el documento y detalles de confianza y de la persona que firma.
Elija Ver > Mostrar/ocultar > Paneles de navegación > Firmas o haga clic en el botón Panel de firma de la barra de mensajes del documento.

¿Que hago si la firma no dispone del tilde verde ?
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 de que aparezca con problemas:

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)

¿Necesito tener firma digital para validar la firma de un tercero?
No

¿Cuál es la autoridad de aplicación ?
La autoridad de aplicación es el Ministerio de Modernización

¿Qué son las autoridades certificantes ?
Son terceras partes confiables que dan fe de la veracidad de la información incluida en los certificados que emiten.

¿Que es PKI?
Se define PKI a la Infraestructura de Firma Digital o Infraestructura de Claves Públicas como el conjunto de normas jurídicas, hardware, software, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones), mediante el uso de certificados digitales como herramienta, se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales.

¿Que es NIST?

Es el Instituto Nacional de Estándares y Tecnología llamada entre 1901 y 1988 Oficina Nacional de Normas es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos que actualmente dispone del programa de validación de módulos criptográficos que impactan en los dispositivos que almacenan los certificados

¿Que es HASH?

Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, 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

¿Quién regula la infraestructura?

La Autoridad de Aplicación establecida en la L ey 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 certificado

Fuentes técnicas

https://es.wikipedia.org/wiki/RSA
https://es.wikipedia.org/wiki/HSM
http://es.wikipedia.org/wiki/X.509
http://es.wikipedia.org/wiki/PGP
http://es.wikipedia.org/wiki/OpenPGP
http://es.wikipedia.org/wiki/Diffie-Hellman

http://es.wikipedia.org/wiki/NNTP
http://es.wikipedia.org/wiki/FIPS_140-2
https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica
https://es.wikipedia.org/wiki/Certificado_digital
https://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n
https://es.wikipedia.org/wiki/Criptograf%C3%ADa
https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica
https://es.wikipedia.org/wiki/Online_Certificate_Status_Protocol
https://es.wikipedia.org/wiki/RSA
https://es.wikipedia.org/wiki/HSM