



Firma Digital

COMO FIRMAR DOCUMENTOS CON TOKEN

Firma digital

Es una herramienta tecnológica que nos permite asegurar el origen de un documento o mensaje y verificar que su contenido no haya sido alterado. Es una secuencia única de letras y números que vincula al firmante con un documento electrónico.

Un documento electrónico firmado digitalmente posee la misma validez jurídica que un documento en papel firmado de puño y letra garantizando de esta manera que no pueda ser objeto de repudio. La firma digital tiene muchas aplicaciones: se la utiliza para hacer trámites con entidades públicas tales como declaraciones impositivas y notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior.

Primero

Instalar el driver del token ⁽¹⁾, de acuerdo al sistema operativo instalado en el equipo que se usará para firmar.

Este pueden obtenerse en: <https://dirinfo.unt.edu.ar/drivers-token/>

Segundo

Instalar la cadena de certificados. La cadena de certificados, que también se conoce como la vía de acceso de certificación, es una lista de certificados que se utiliza para autenticar una entidad.

La cadena puede obtenerse en: <https://dirinfo.unt.edu.ar/drivers-token/>

Instalar un programa que permita firmar

Como por ejemplo Adobe Acrobat Reader DC, que es una versión gratuita. Puede obtenerse en:

<https://get.adobe.com/es/reader/>

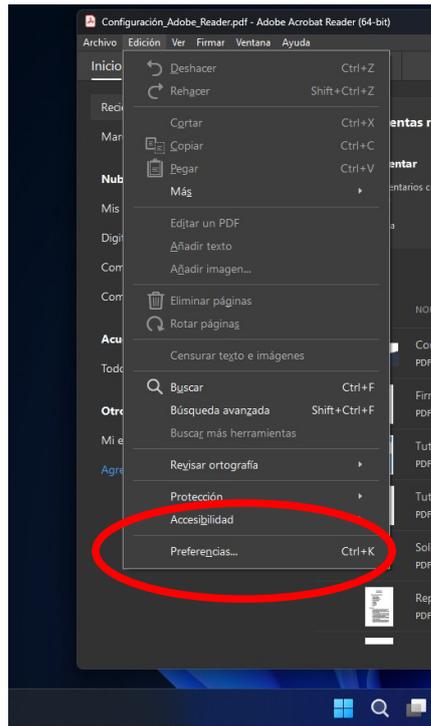
¹ El driver debe ser el adecuado para el modelo de token.



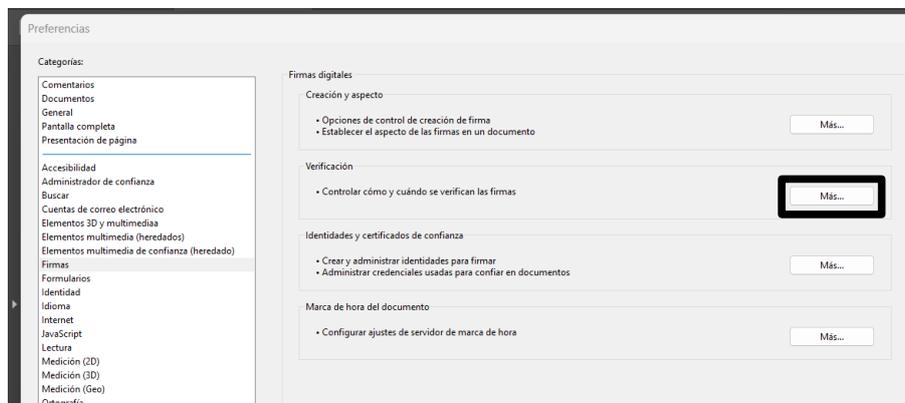
Firma Digital

Como configurar Adobe Acrobat Reader DC para firma Digital

Ir a Edición → Preferencias



Hacer click en **Firmas** y luego en el botón **Más...** de Verificación





Firma Digital

Preferencias de verificación de firma

Verificar firmas al abrir el documento

Cuando el documento tenga firmas válidas que no hayan sido identificadas como de confianza, preguntar si se desea ver los firmantes e indicar si son de confianza

Comportamiento de verificación

Al verificar:

Utilizar el método especificado por el documento; avisar si no está disponible

Utilizar el método especificado por el documento; si no está disponible utilizar el método predeterminado

Utilizar siempre el método predeterminado: Seguridad predet. de Adobe

Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible

Usar marcas de hora caducadas

Ignorar información de validación de documento

Hora de verificación

Verificar firmas mediante:

Hora en la que se creó la firma

Hora segura (marca de hora) incrustada en la firma

Hora actual

Información de verificación

Agregar automáticamente información de verificación al guardar PDF firmado:

Preguntar cuando la información de verificación es demasiado grande

Siempre

Nunca

Integración de Windows

Confiar en TODOS los certificados raíz del almacén de certificados de Windows para:

Validar firmas

Validar documentos certificados

La selección de cualquiera de estas opciones puede provocar que cualquier material se trate como contenido de confianza. Tenga cuidado antes de habilitar estas funciones.

Ayuda Aceptar Cancelar

La configuración debe quedar con las casillas de verificación y botones marcados como se indica en esta imagen.