

El Documento Nacional de Identidad electrónico (DNle)

permite operar en internet y realizar gestiones telemáticas con las máximas garantías de seguridad, acreditando electrónicamente la identidad de los ciudadanos y posibilitando la firma de transacciones electrónicas ante las Administraciones Públicas y ante otros prestadores de servicios que participan de la firma electrónica.

Para más información, se puede consultar la página web:

www.dnielectronico.es

O llamando al teléfono gratuito de información:

900 364 463



Dirección General de la Policía



DNI ELECTRÓNICO IDENTIFÍCATE CON ÉL



¿Qué incluye el DNle?

El DNle incluye los mismos datos de identificación personal que hasta ahora, junto con un chip electrónico que contiene los datos personales y la fotografía del titular, la imagen digitalizada de su firma manuscrita y el patrón de la impresión dactilar. Igualmente, incorpora los certificados electrónicos de autenticación y firma electrónica.

¿Qué son los certificados electrónicos?

Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firma a su titular y confirma su identidad.

Funciones básicas

El DNI electrónico desarrolla dos funciones básicas:

- Acreditar la identidad, físicamente y por medios telemáticos, de un ciudadano frente a terceros.
- Poder realizar acciones electrónicas con plena validez legal, garantizando la identidad de los intervinientes en la acción.

Para ello, el DNle contiene un **certificado de autenticación** y un **certificado de firma electrónica reconocida**.

Usos de los certificados

Los Certificados de Identidad Pública, emitidos por la Dirección General de la Policía (Ministerio del Interior) e incorporados al chip, tienen como finalidad:

Certificado de autenticación: Garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El certificado de autenticación asegura que la comunicación electrónica se realiza con la persona que dice que es.

Certificado de firma: Cada firma electrónica cuenta con dos claves, una **pública** y otra **privada**. Toda la información que cada titular envíe a través de medios telemáticos estará asociada automáticamente a su clave privada —que sólo conoce él—, mientras que los posibles receptores conocerán únicamente su clave pública.

Clave de acceso personal -PIN-

Al recibir el nuevo DNI, cada titular obtendrá una clave personal de acceso (PIN), similar a las de las tarjetas de crédito, necesaria para el uso de los certificados electrónicos incluidos en su DNle. El PIN garantiza la confidencialidad de la información contenida en el chip del documento.

El titular del DNI podrá cambiar su PIN en cualquier momento y cuantas veces lo desee, ya sea a través de INTERNET (en la dirección www.dnielectronico.es) o en las Oficinas de Expedición del DNI. El PIN debe tener un mínimo de ocho y un máximo de dieciséis caracteres (letras, números o símbolos).

Al activar su firma electrónica, recibirá un sobre con su clave personal (PIN) y una serie de consejos sobre la misma que les recomendamos tengan en cuenta.

Ante cualquier duda, puede llamar al Centro de Atención al Ciudadano **900 364 463**, o visitar la web www.dnielectronico.es

¿Cómo se utiliza el DNI electrónico?

Para la utilización electrónica del DNle, se necesita disponer de un ordenador con conexión a la red y un lector de tarjetas. La primera vez que utilice el DNle, el titular debe descargar un software propio de acceso a la tarjeta, disponible en la web www.dnielectronico.es

Su forma de uso es sencilla. Tras conectarse al sitio web deseado y siguiendo las instrucciones del prestador del servicio, el titular pasará su DNle por el lector para acreditar su identidad. Esta operación se realizará igualmente a la hora de firmar electrónicamente el documento que acredite la firma del titular cuando le sea requerido.

El prestador de servicios puede acceder al Servicio de Validación para comprobar que el Certificado electrónico del usuario no ha sido suspendido o revocado.

Igualmente, es conveniente que el prestador de servicios proporcione al usuario algún elemento de garantía de No Repudio y Autenticidad de Destino (Semejante a un certificado digital de haber realizado la transacción).

Validez de los certificados

Con independencia de la validez del DNI, los certificados electrónicos reconocidos incorporados al mismo tendrán un período de vigencia de treinta meses. A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente.

La pérdida de validez del Documento Nacional de Identidad (por caducidad, pérdida, sustracción o deterioro de la tarjeta) llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

En caso de pérdida o robo, comuníquelo con la mayor inmediatez a la Dirección General de la Policía a través de las Oficinas de Expedición del DNI o de las Comisarías de Policía, con el fin de que puedan ser revocados los certificados electrónicos incorporados al mismo.

