

7.1. certificado digital

Para poder realizar firma electrónica necesitamos tener un **certificado digital**. Este certificado es el que acredita nuestra identidad en Internet.

El certificado autentica, mediante una pareja de claves en un fichero software o en tarjeta la identidad del firmante.



Com identificar-me

Certificat Digital

Necessitaréu un certificat digital reconegut pel Govern de les Illes Balears. [Més informació](#)

Inicia

Ejemplo de certificado electrónico



Cómo conseguir un certificado

Estos certificados se pueden conseguir de varias formas:

- El propio DNI electrónico contiene un certificado digital que podemos utilizar.
- Algunos organismos como la FNMT (Fábrica Nacional de Moneda) también nos pueden hacer un certificado digital.

El certificado autentica, mediante una pareja de claves en un fichero software o en tarjeta la identidad del firmante.

Autoridades de certificación

Estos certificados, son emitidos por una entidad emisora de certificados que **dan fe de que el portador del certificado es quien dice ser**.

Existen varias autoridades de certificación:

- FNMT
- Agencia de Tecnología y Certificación Electrónica de la Generalitat Valenciana
- Agència Catalana de Certificació
- Dirección General de la Policía (para el DNI), etc.

Tipos de certificados

Las entidades certificadoras expedan distintos tipos de certificados, dependiendo de si el solicitante es:

- Un ciudadano
- Un representante de una empresa (persona jurídica, de entidad sin personalidad jurídica y, para administradores únicos y solidarios)
- Un empleado público

Si disponemos de un certificado y quieres comprobar su validez, firmar, visualizar o validar una firma puedes utilizar los servicios del portal de firma electrónica.

¿Cómo conseguir un certificado digital?

Paso 1. Realizar una solicitud online.

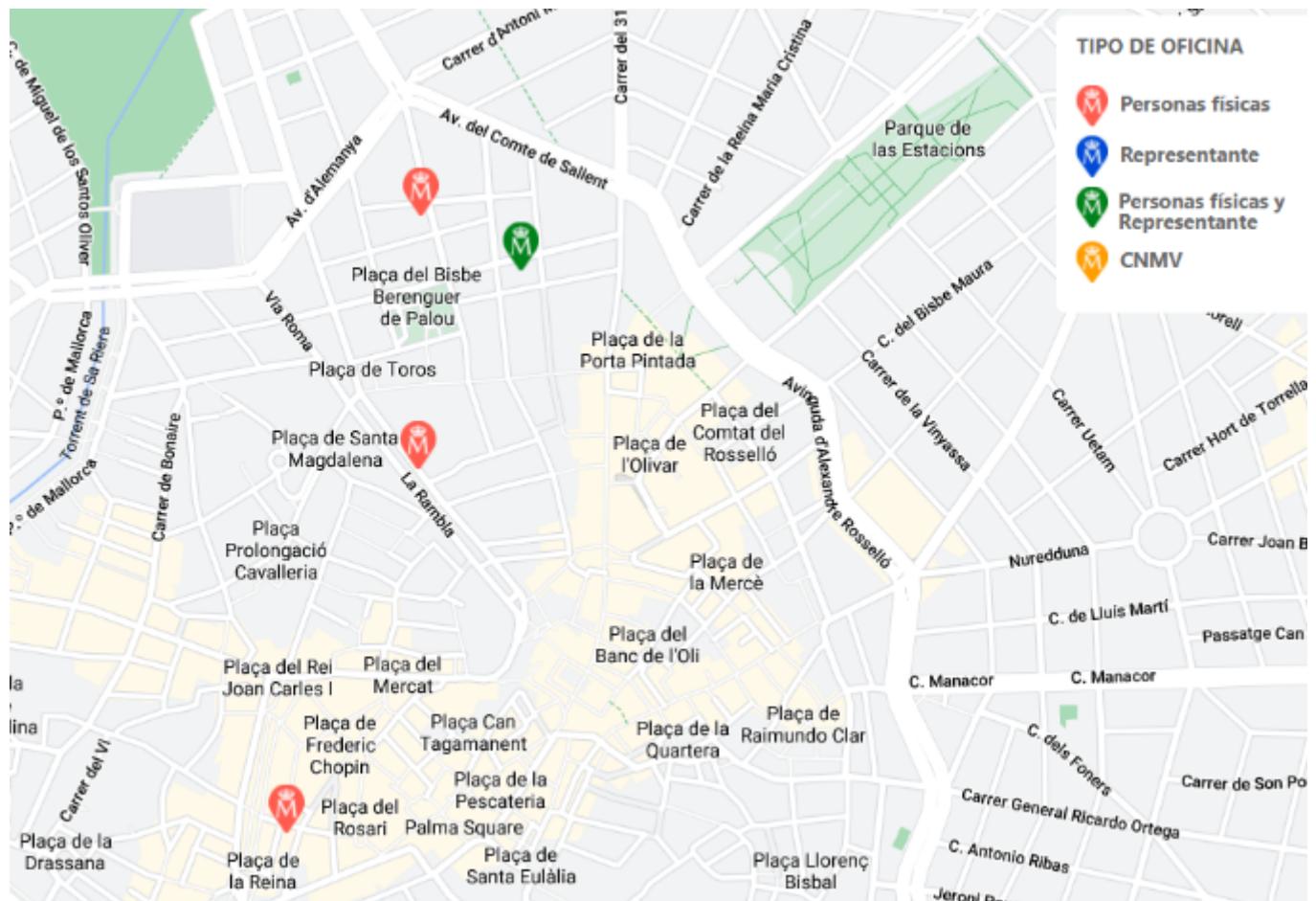
- Desde el **ordenador** donde queremos instalarlo.
- Utilizando el **navegador** que queramos.
- Al final de este proceso se obtiene un código que será necesario para poder acreditar tu identidad.



Paso 2. Acreditar identidad

- Presentarse en una Oficina de Registro para acreditar tu identidad.
- Para el DNI tendrás que personarte en las oficinas de la D. G. de la Policía

<http://mapaoficinascert.appspot.com/#>



Paso 3. Descargar certificado

- Antes realizar el registro presencial
- Tenemos que tener del código obtenido en el primer paso
- Con esto podremos descargar el certificado vía Internet.
- El certificado quedará instalado en ese navegador y PC utilizado



Utilización

La mayoría de administraciones públicas tienen un portal telemático en el que realizar trámites y solicitudes, utilizando el certificado electrónico o la clave para identificarnos.



Una vez entremos, si tenemos nuestro certificado digital instalado, nos permitirá seleccionarlo (podríamos tener varios en el equipo).



DNI Electrónico

Introducción y curiosidades

Hay que remontarse hasta el año 1944 -en plena época franquista y en los últimos coletazos de la Segunda Guerra Mundial- para conocer el origen de este documento.

Entró en funcionamiento un 2 de marzo: los primeros documentos de identidad no portaban fotografías y, por tanto, resultaba complejo reconocer y dar con algunas personas.

Los tres primeros números le correspondieron a Franco y su familia



Del 10 al 99, reservados para miembros de la Casa Real. Además, no existe el número 13 en los DNIs -por superstición.

Primer DNI informatizado

El primer DNI informatizado regulado por Orden del ministerio del Interior de fecha 12 de julio de 1990.

No figura impresión dactilar y si dos líneas de caracteres OCR.



Primer DNI electrónico

Primer DNI que incorpora CHIP, convirtiendo al Documento Nacional de Identidad en un documento electrónico.

Se trata además de una tarjeta de policarbonato grabada con láser, con las mismas medidas que una tarjeta de crédito convencional.

Permite la conexión a servicios telemáticos, a través de un lector de tarjetas conectado al ordenador.



Máquina para crear DNI



DNIe



—El DNIe es el carnet de identidad de siempre, con un chip incluido en su interior. Este chip guarda información nuestra que nos permite utilizarlo también para autenticarnos en Internet. —

¿Qué podemos hacer con el DNIe?

Este DNI aparece el 2006 y se fabrica hasta el 2015.

El DNIe me permite:

1. Acreditar electrónicamente identidad
2. Firmar digitalmente documentos electrónicos



¿Qué información contiene el chip?

El chip integrado contiene la siguiente información nuestra:

- Datos personales
- Fotografía
- Firma digitalizada
- Huella dactilar
- Certificados de autenticación y firma electrónica



DNI 3.0

El DNI 3.0. nació en enero del 2015

Incorpora las mayores y más sofisticadas medidas de seguridad que hacen virtualmente imposible su falsificación.

Disponer de un chip dual-interface que permite su utilización con contacto y también modo contactless (NFC)

Elimina la necesidad de un lector de tarjetas o drivers, facilitando la conexión online y la autenticación del ciudadano.



https://www.dnielectronico.es/PDFs/Historia_de_los_documentos_de_identidad.pdf





Lector de teclado



Lector USB

DNie

Para poder utilizarlo necesitaremos un PIN que nos proporcionarán en la DGP. Si lo olvidamos, tendremos que ir presencialmente a conseguir otro.

También necesitaremos:

- Lector de tarjetas
- Software de acceso a la tarjeta



PIN

El PIN es la contraseña personal que cada DNI electrónico tiene asociado. Se nos entrega en el momento de expedición del DNIe, en un sobre sellado.

No podemos cambiar el PIN por Internet. Si que queremos es modificar nuestro PIN o incluso obtenerlo de nuevo en **Puntos de Actualización del DNI (PAD)**. No es necesario que pidamos cita previa

Podremos hacerlo nosotros mismos a través de las máquinas que se encuentran a disposición de los ciudadanos

¿Qué podemos hacer?

- Consultar datos personales
- Vida laboral
- Puntos tráfico
- Empadronamiento
- Trámites
- Declaración renta
- Pago tasas
- Desempleo
- Servicios con empresas
- Banca online
- Firma de contratos



Pagar tasas o impuestos

El DNIE o el certificado electrónico nos permiten también pagar tasas (por ejemplo, para que nos den un título o certificado de estudios) o impuestos.

En Baleares, existe la Agencia Tributaria o **Atib** donde podemos pagar nuestros impuestos, tanto presencialmente en sus oficinas como online a través de su **sede electrónica**.

Lectores

Los tipos de lectores más habituales son:

- Lector USB conectado a un ordenador
- Teclado especial con lector integrado
- Smartphone mediante la tecnología NFC
- La necesidad de tener este hardware ha sido uno de los principales problemas a la hora de implantar el DNI electrónico

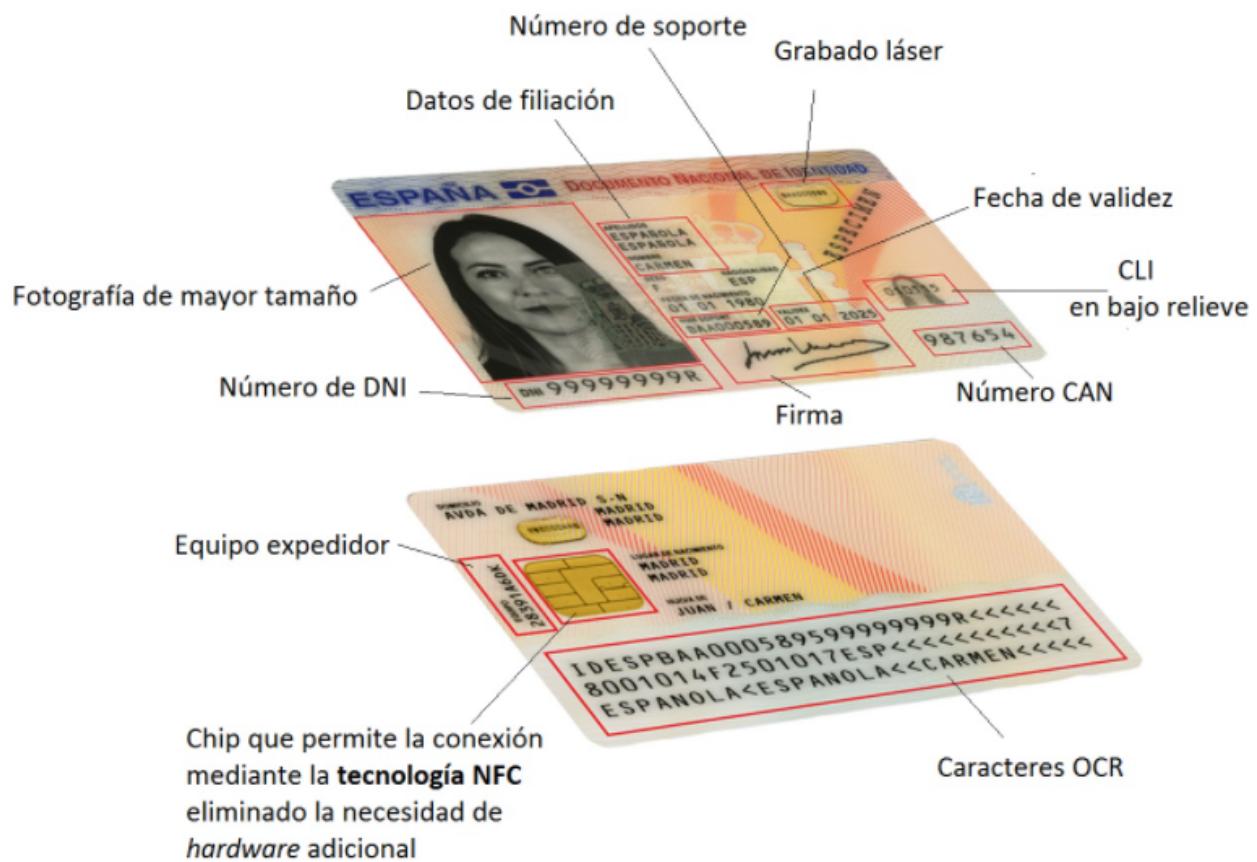


<https://www.youtube.com/watch?v=kTC-xxdTufA>

Partes DNIE



El **DNIe 3.0** incorpora un chip *dual interface*, que permite la conexión mediante contacto o de forma inalámbrica mediante tecnología NFC.



Firma digital

La firma digital viene a sustituir a la manuscrita en el mundo de la informática. Es decir, si firmamos de forma digital un documento, le estaremos dando veracidad y como sucede con la firma manuscrita, no podremos decir que no lo hemos firmado nosotros; por lo tanto, seremos responsables de lo que en él se diga.

¿Para qué sirve la firma electrónica?

La firma digital viene a sustituir a la manuscrita en el mundo de la informática.

- Si firmamos de forma digital un documento, le estaremos dando **veracidad**
- No podremos decir que no lo hemos firmado nosotros
- Seremos responsables de lo que en él se diga.

Una firma electrónica es un conjunto de datos electrónicos que:

- Se adjuntan a un documento electrónico determinado
- Identifican al firmante de manera inequívoca
- Certifican la integridad del documento
- Aseguran que el firmante no puede repudiar lo firmado.

Mecanismo

La descripción del mecanismo de firma electrónica es el siguiente texto:

Paso 1. Creamos el documento

La firma electrónica es un concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta el contenido de un mensaje electrónico a través de cualquier medio electrónico válido. Ejemplos:

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes: Código secreto o de ingreso: es la necesidad de una combinación determinada de números o letras, que son sólo conocidas por el dueño del documento, o lo que todos usamos, por ejemplo, en los cajeros automáticos, es el famoso PIN (Personal Identification Number).

Métodos basados en la Biometría: se realiza el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz). En el perfeccionamiento del cifrado de mensajes, llegamos a lo que se conoce como criptografía.

Paso 2. Calculamos el hash

Se calcula un valor resumen del documento, conocido como **hash**, utilizando algún algoritmo como el **SHA 256**.

8D1DA152769DA821009BBB2D6DD856DE

!!! note

Al estar calculado con SHA256, el hash tiene 256 bits (0s y 1s), que se pueden representar con 64 dígitos hexadecimales.

Paso 3. Firmamos el hash con nuestra clave privada

Este valor resumen se cifra utilizando nuestra **clave privada**.

!!! note

Recordemos que nuestra clave privada nunca sale de nuestro dispositivo, únicamente la pública.

```
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA0CUu5s7oUYtm1k/XLY0tPU0QaBAirTQ8Rc  
T/Mn/JQCmyoQh8nrhb3IB93WRR5+mmzaa6WFU7TJyM7J0+VWTm0QIDAQABAkAwMuwRdohFmcpOh16Fo6BS  
0a466sGc6i0q5FtUD1NED/iu8urdmKi24r+8mnykcGadZIXcnH+ti3GOfdW/dTIhAiEA9uZW7uD1eaVzyH  
eLDyswOV1j8bCCSLUQbpWxXp6E488CIQDX0StiAkGhT9Ju9wRsdHDoakUoc2xywoswY+MH1xQTXwIhAMnZ  
mJrlCwsxS85JhUOacGuFoW73ehwNA2kVMpQDjutbAiA4/+CiYRAuZ60fdRQxBMvxRmf/mASThrg2Tpterb  
p6pwIhAJMFoBU4zGYBm3UQ0jZkRXNtxKzsJODtmNgZwYvdJZkd
```

El resultado de este valor es lo que se conoce como firma digital del documento.

```
sfsvMBz4Rdr00Ce1naThF0ZkESDW0fjIpXf3GQchsDpkvc7oI5IowPu6Yefqr305LTu5pc0RoHoaJzMN5E  
MaHA==
```

Esto permite asegurar que la única persona que ha podido firmar el documento soy yo, el único que conoce la clave privada.

Envío

El documento firmado contendrá:

1. El contenido del texto original
2. La clave pública de la persona que ha firmado
3. La firma digital

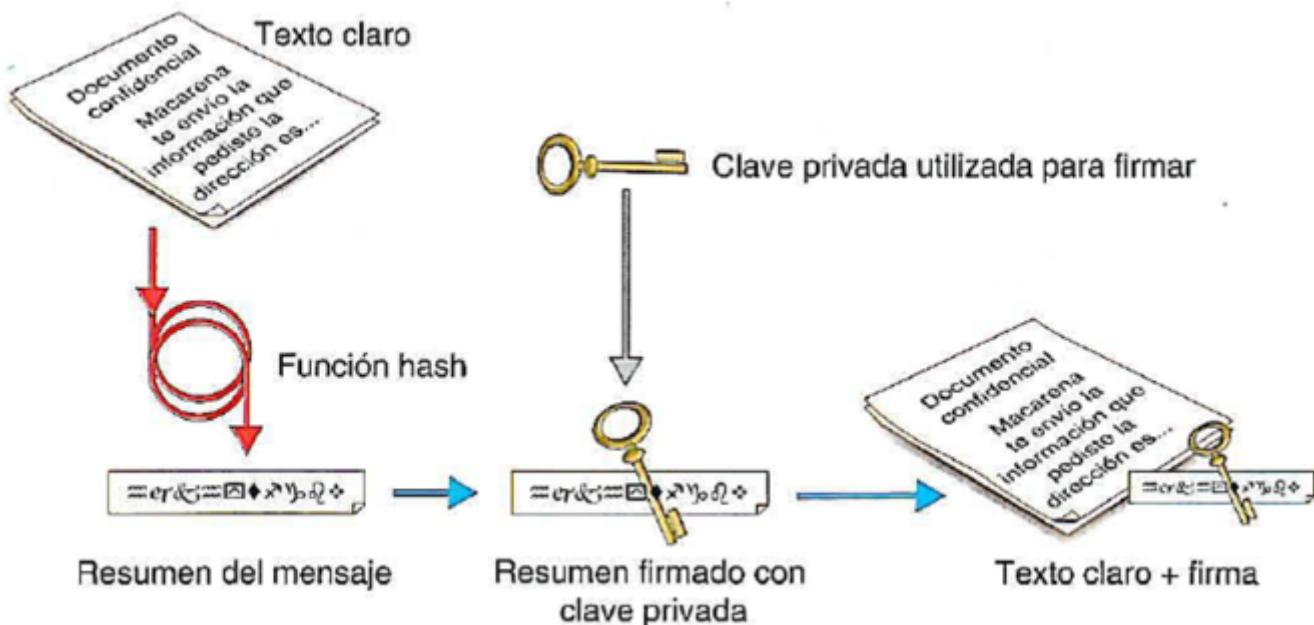
Con estos 3 elementos, en cualquier momento podemos comprobar que la firma es auténtica.

Firma de documentos electrónicos

Si contamos con un **certificado digital**, podemos comenzar a firmar documentos. La firma electrónica en documentos se puede realizar de dos formas:

- Online, a través de un servicio de verificación y generación de firmas electrónicas como es VALIDe

- A través de aplicaciones de firma electrónica o de ofimática que, tras ser descargadas y ejecutadas en un ordenador, permitirán realizar firmas de documentación sin la necesidad de estar conectado a Internet.



Sellado en el tiempo

Una de las características más útiles que puede ir asociada a la firma electrónica es lo que se conoce como "sellado en el tiempo". Se trata de un método para probar que un conjunto de datos (en este caso, la firma que se ha realizado) existió en un momento determinado (fecha y hora).



Identidad digital



identidad

nombre femenino

1. Circunstancia de ser una persona o cosa en concreto y no otra, determinada por un conjunto de rasgos o características que la diferencian de otras.
"crisis de identidad"
2. Conjunto de rasgos o características de una persona o cosa que permiten distinguirla de otras en un conjunto.
"nunca revelará su verdadera identidad"

Identificación

En nuestro día a día, necesitamos identificarnos para acceder a servicios. Es decir, demostrar que somos nosotros realmente.

Las formas de identificación más comunes son el DNI, el pasaporte, la tarjeta de crédito o el carnet de conducir. Todas estas formas sirven para poder acceder a servicios bancarios, alojamientos, transporte,

compras en línea, entre otros. Además, muchos lugares también requieren la presentación de un documento de identificación para poder acceder a ellos.

En el mundo real la verificación relacionada con

- Rasgos (aspecto físico)
- Datos (huella dactilar)
- Firmas (firma en documentos)



Pero en el mundo digital, la autenticación se basa en otros métodos como:

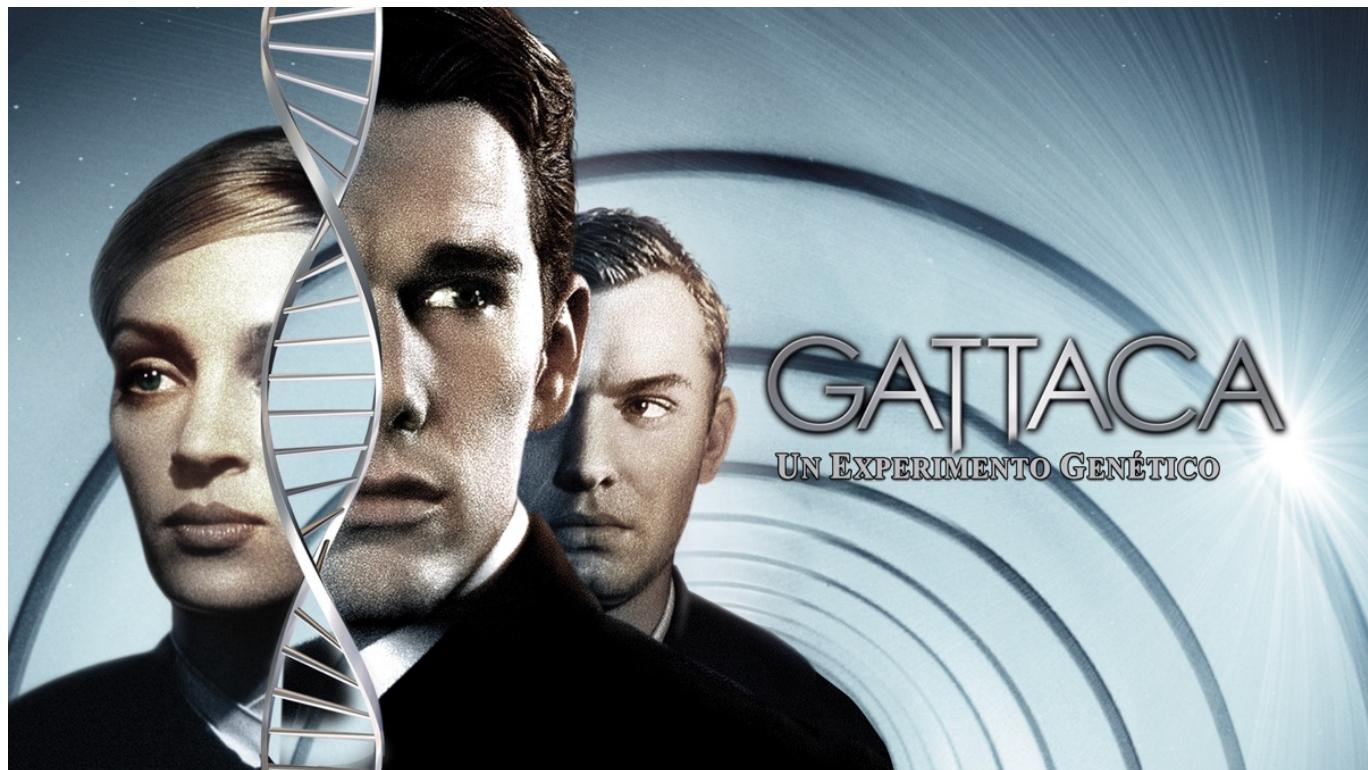
- Contraseñas
- Códigos de seguridad
- Token de autenticación
- Biometría
- La autenticación de dos factores (2FA)



HUELLA DACTILAR



Las huellas digitales son únicas, incluso para estos hermanos idénticos. Esto se debe a que las huellas dactilares no responden a la genética sino que, al formarse al tercer mes de embarazo, van variando cuando los dedos rozan con el cordón umbilical o este crece permitiendo más movimientos intrauterinos



Firma

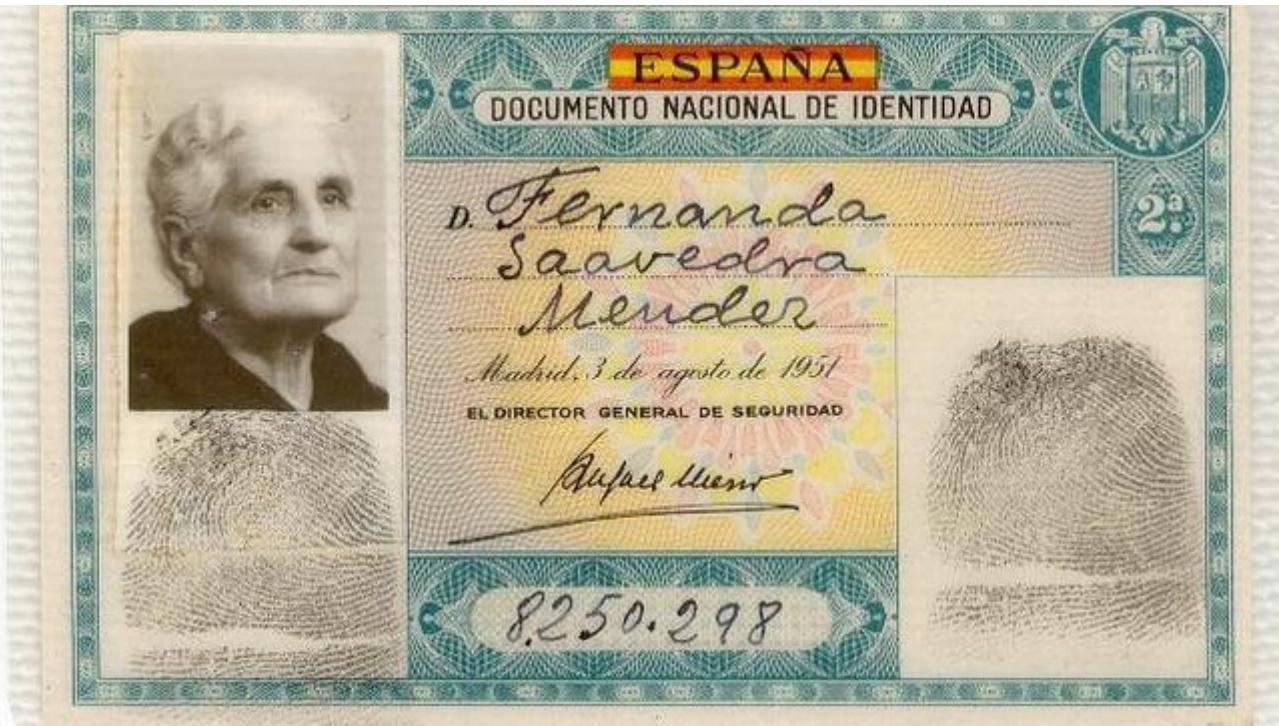
La firma de una persona es una forma de identificación. No es una forma válida de autenticación en sí misma, ya que no es una prueba de quién es la persona. Para ser válida, la firma debe ser autenticada por un tercero, como un notario público, y debe estar asociada con un documento legalmente vinculante.

Jane Doe Plan & Buffet
Bill Gates
May T M Gail Winfrey



<i>Juan González</i>	CON LETRAS MUY PEQUEÑAS EGOÍSTA, TACAÑO
<i>JG</i>	CON LETRAS GRANDES SOÑADOR, INDEPENDIENTE, INGENUO, POCO PRÁCTICO, CONFIANZUDO, BONDADOSO
<i>Juan González</i>	CON LETRAS REDONDAS BONDADOSO, SUTIL, TRANQUILO
<i>Juan González</i>	ANGULADA IMPULSIVO, IRRITADO, INDEPENDIENTE, QUIERE AUTOAFIRMARSE
<i>Juan González</i>	CON LETRAS JUNTAS LÓGICO, RACIONAL, CONSERVADOR
<i>Juan González</i>	CON LETRAS SEPARADAS FLEXIBLE, CON HABILIDAD DE ADAPTARSE, BUSCA HACER SUS SUEÑOS REALIDAD
<i>Juan González</i>	ADORNADA JACTANCIOSO, TIENDE A ADORNAR LA REALIDAD, FALSO
<i>Juan González</i>	«AL DESNUDO» LÓGICO, DE PENSAMIENTO CONCISO
<i>J. González</i>	COMPACTA TÁCTICO

DNI



Documento nacional de identidad



La forma más habitual de demostrar nuestra identidad es presentar nuestro DNI o firmar.

La policía nos da un DNI solo a nosotros, con nuestra huella, foto y firma.

Presentando este documento con nuestra foto, demostramos que nuestros datos son los que allí figuran.

¿Por qué 23?

Probablemente pienses que se divide el número de identificación entre 23 porque una buena mañana a alguien le dio por hacerlo así, pero tiene su explicación. Si te fijas en la fila de las letras en la tabla de arriba, verás que **coincide con el abecedario**, pero que solo hay 23 letras de 27. **¿Dónde están las letras que faltan?** Se han eliminado a propósito. Las razones son las siguientes:

- La Ñ (eñe) se puede confundir con la N (ene).
- La vocal I se confunde con un 1 (uno) o la L (ele) minúscula.
- La vocal O se confunde con el O (cero).
- La vocal U se confunde con la V (uve).

¿Cómo nos identificamos en Internet?

En la actualidad, muchas de las tareas que antes se realizaban de forma presencial ahora se han trasladado al ámbito **digital**, ya sea por comodidad o por imposición legal. Esto conlleva una necesidad de encontrar una forma de acreditar de manera segura nuestra identidad, ya que no podemos mostrar físicamente un documento de identidad como el DNI.

Contraseñas

La contraseña es el método más ampliamente extendido para proteger nuestros datos, permitiendo una identificación y acceso seguros a nuestra información. Aunque no es el método más seguro, hay algunos elementos clave que debemos tener en cuenta para mejorar su seguridad: utilizar contraseñas largas y complejas, incluir caracteres especiales, mayúsculas o minúsculas, cambiar la contraseña de forma regular y no utilizar la misma contraseña para varias páginas.

Además, es conveniente contar con métodos de recuperación, como un número de teléfono o dirección alternativa, para poder recuperar el acceso si olvidamos la contraseña.



A graphic titled "Hacker's Top 10 List of Most Used Passwords". It features a cartoon illustration of a hooded hacker on the left. The title is in large white font on a red background. To the right are three red star icons and a yellow warning sign with an exclamation mark. Below the title is a table showing the top 10 most used passwords. To the right of the table is a section titled "Here's how often the 10 most common passwords in different countries match the Hacker's Top 10 list:" with five donut charts showing percentages for Worldwide, USA, Spain, Italy, Russia, Germany, and France.

Rank	Password	Rank	Password
1	123456	6	654321
2	password	7	111111
3	12345678	8	123123
4	1234567	9	1234567890
5	qwerty	10	Iloveyou

Here's how often the 10 most common passwords in different countries match the Hacker's Top 10 list:

- Worldwide: 80%
- USA, Spain: 50%
- Italy, Russia: 33%
- Germany: 25%
- France: 10%

Formas de demostrar nuestra identidad

Existen multitud de métodos de demostrar nuestra identidad digitalmente:

1. DNIe
2. Certificado digital
3. Contraseñas
4. Biometría

Algunas simplemente sirven para proteger algo, y otras demuestran que somos una persona concreta.