



UNIDAD 23: INTERNET. LA ADMINISTRACIÓN ELECTRÓNICA.



Contenido

1. INTERNET.....	2
1.1 El protocolo TCP/IP	2
1.2 Dirección IP	4
1.3 Nombres de dominio	4
1.4 Servicios de Internet	5
1.5 La web.....	6
1.6 Los navegadores.....	6
1.7 Buscadores	6
1.8 Comunicación a través de internet. Telefonía IP. Videoconferencia	7
2. LA ADMINISTRACIÓN ELECTRÓNICA	8
2.1 Firma electrónica y certificados digitales.....	9
2.2 El DNI electrónico	11



1. INTERNET

Internet nace a finales de los años 60 como un proyecto militar para permitir la interconexión de distintos ordenadores entre sí más allá de un equipo con sus mismos componentes (como sucedía con los ordenados principales de los departamentos militares, que utilizaban el protocolo SNA para interconectarse con las impresoras, las cintas donde se grababa la información o los terminales para la introducción de datos).

El paradigma sobre el que se inició Internet, conocido como ARPAnet, estaba basado en que un ordenador podía ofrecer sus servicios (es decir, actuar como servidor) que eran consumidos por otros equipos (denominado clientes). A este paradigma se le denomina paradigma cliente-servidor.

Además, dado que debía poder funcionar en condiciones adversas fruto de un conflicto bélico, era responsabilidad de cada uno de los intervinientes asegurarse que el sistema funcionaba en dichas condiciones adversas, puesto que la red podía no ser fiable en cuanto a su calidad.

En aquella misma época, se empezó a elaborar por la empresa ATT y luego por la Universidad de Berkeley, un sistema operativo denominado UNIX, que permitía ser ejecutado sobre distintos tipos de ordenadores. UNIX incorporaba desde el inicio los protocolos de comunicación de la red DARPA (o ARPA Net). Este sistema operativo se empleó por gran número de entidades, desde grandes empresas a instituciones educativas, y por lo tanto permitiendo su conexión a la Red.

Dado el alto número de instituciones académicas norteamericanas que formaban parte de Internet en aquella época, el Gobierno USA decidió transferir la gestión de Internet a una agencia académica (la NSF, National Science Foundation, Fundación Nacional para las Ciencias).

Simultáneamente, un cierto número de empresas empezaron a ofrecer sus servicios en Internet, fundamentalmente empresas del sector de la informática y las comunicaciones.

En España, las principales universidades procedieron a constituir un equipo (RedIRIS) que estableció la primera interconexión de redes y de estas con Internet en la segunda mitad de los años 80, mientras que el acceso comercial se producía a través de un único prestador de servicios. En 1995, el Instituto Nacional de Estadística y el Boletín Oficial del Estado fueron los dos primeros organismos de la Administración General del Estado en conectarse a RedIRIS y, por tanto, a Internet.

Precisamente, en dicha época, Microsoft implementó el protocolo TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet) en su sistema operativo Windows XP, produciéndose el comienzo del acceso del gran público a Internet.

En definitiva, lo que comenzó siendo una conexión entre iguales de un centenar de ordenadores ha dado lugar a la mayor interconexión de ordenadores, teléfonos móviles y redes de ordenadores a nivel mundial.

1.1 El protocolo TCP/IP

Cuando se desarrolló Internet, el conjunto de ordenadores era de muy distintos fabricantes. Por ello, fue preciso desarrollar un modelo que describiese todos los protocolos por los que se iban a interconectar entre sí.

Estos protocolos son bastante complejos, por lo que se decidió establecer un modelo basado en capas, cada una con una función, y en el que cada capa recibe los datos que han sido preparados por la capa superior y se entregan, tras ser procesados, a la capa siguiente.

El modelo TCP/IP establece 4 capas (aunque la primera de ellas está subdividida en dos, lo que

podría dar lugar a entender que tiene 5 capas)

Las capas de más física a más abstracta son:



- ☐ Capa 1, de acceso al medio, que comprende dos subcapas:
 - La subcapa física que se encarga de las labores de más bajo nivel referidas al cableado, o a la antena en las comunicaciones inalámbricas.
 - La subcapa de enlace, que adapta la información proveniente de capas superiores al interfaz por el que vaya a ser enviada. De esta manera, solo esta capa es la que sabe si está utilizando una red WiFi o Bluetooth para conectarse con Internet.
- ☐ Capa 2 o Capa de Internet: Esta capa es la que se encarga de identificar a cada una de las máquinas ante el resto de las máquinas conectadas a Internet, mediante una dirección única.
- ☐ Capa 3 o capa de transporte: Esta capa se encarga de la emisión o recepción de la información entre dos máquinas identificadas mediante las direcciones IP asignadas en la capa 2. Como la información a transmitir puede ser muy Voluminosa, esta capa la divide en paquetes que se envían por dos medios de transporte:
 - TCP, en el que el emisor espera recibir confirmación de la correcta recepción por parte del receptor antes de seguir mandando más paquetes.
 - UDP, en el que el emisor envía los paquetes y el receptor reconstruye la información con los paquetes que hayan llegado.
- ☐ Capa 4 o capa de aplicación: En esta capa, cada ordenador (o móvil o televisión inteligente,...) ejecuta el programa de comunicaciones asociado al tipo de comunicación (correo, WhatsApp, transferencia de ficheros, navegación Web,...). Existen dos tipos de aplicaciones:
 - Servidor: Es una aplicación ejecutándose en un ordenador que proporciona sus servicios al resto de ordenadores. Por ejemplo, Youtube es un conjunto de servidores que transfieren videos al resto de equipos que se lo solicitan.
 - Cliente: Es una aplicación que se ejecuta en los ordenadores de los usuarios y que consumen los servicios ofrecidos por los servidores. En el ejemplo anterior, pueden ser tanto un navegador como la aplicación específica para móviles.



1.2 Dirección IP

Antes de hablar del direccionamiento IP, vamos a hablar de otro tipo de direccionamiento.

Como ya hemos comentado, existe una subcapa, la de enlace, que forma parte de la capa de Acceso al medio, que se encarga de ocultar al resto los aspectos físicos de la transmisión.

En esta capa, cada uno de los interfaces tiene un identificador único, denominado dirección MAC, de las siglas en inglés de control de acceso al medio (Media Access Control) y que, en principio, es inmutable. Está formada por 48 bits, que se agrupan en seis bloques de dos caracteres hexadecimales, por ejemplo F4:60:E2:C5:D5:51, en el que los tres primeros se asigna por una organización (IANA) al fabricante y los tres siguientes son establecidos por el propio fabricante.

¿Por qué se utilizan esta dirección existiendo IP? Por ejemplo, imaginemos que tenemos una tableta con WiFi. El fabricante, a priori, no sabe con qué operador vamos a tener WiFi. Sería francamente engorroso que tuviésemos que ir a un servicio técnico para que pudiera cambiarnos de dirección y pudiésemos continuar navegando si voy a un hotel. De esta manera, la tableta se entenderá con el punto de la red WiFi y este le proporcionará la dirección IP única.

La dirección IP es un conjunto de 32 bits que identifican de manera única un ordenador en una red TCP/IP, en su versión IPv4. Esto podría dar lugar a más de 4 mil millones de direcciones y, por tanto, de equipos. Sin embargo, el gran crecimiento han dejado prácticamente exhausta la numeración IPv4 por lo que se ha establecido una nueva numeración, denominada IPv6, que mediante 128 bits, permite cerca de 340 sextillones (millones de millones de millones de millones de millones de millones) de direcciones IPv6.

Las direcciones IPv4 se presentan, para ser legibles por humanos, presentando los bits agrupados en 4 bytes, como 172.16.0.19.

Para incorporar el direccionamiento IPv6, se reservaron direcciones IP cuando estas no debían ser visibles en el exterior de una organización. Estos rangos son 10.0.0.0/8, 172.16.0.0/16 y 192.168.0.0/24. Los sufijos /8, /16 y /24 indican el número de bits que tienen en común dos redes distintas. En las Administraciones Públicas españolas se usan grupos de direcciones de la red 10.0.0.0/8 asignadas por la Secretaría General de Administración Digital.

Si una organización debía conectarse con otra y se podía producir una “colisión” entre dos direcciones IP o era necesario que una dirección IP fuera visible fuera de la organización, se estableció un mecanismo denominado NAT (Network Address Translation”, Traducción de Direcciones de Red).


Además, algunas máquinas no necesitan una dirección todo el tiempo, sino solo cuando se conectan. Por ello, existen dos tipos de direccionamiento:

- ☐ Estático, en el que la dirección IP se asigna de manera permanente.
- ☐ Dinámico, en el que la dirección IP se asigna por un tiempo limitado (que puede ir de varias horas a varios días) y que, si el ordenador está encendido en los momentos previos a que expire, son renovados por idéntico tiempo.

1.3 Nombres de dominio

Es bastante poco práctico acceder a los servicios de un ordenador mediante la dirección IP de ese ordenador, siendo mucho más fácil memorizar nombres.

Para ello, se diseñó el Sistema de Nombres de Dominio, DNS por sus siglas en inglés, Domain Name System. Los nombres de las máquinas incluyen el nombre de la organización a la que



pertenecía la red y, en su caso, el código del país, todo ello separado por puntos.

No existe una limitación al número de elementos separados por puntos, pero se ha de tener en cuenta que el nombre completo, incluyendo los puntos, debe tener como máximo 64 caracteres.

Se denomina dominio a los últimos dos, o en ocasiones, tres grupos de elementos. Así, en www.google.com, el dominio es google.com.

Se denomina dominio de primer nivel al último elemento (el más a la derecha del nombre). Son de dos tipos:

- ☐ Geográficos, con el código ISO del país que gestiona el dominio: .es para España, .fr para Francia, .de para Alemania, etc...
- ☐ No geográficos, en los que una entidad gestiona el dominio. Aquí hay dos grupos, el histórico (.com, para empresas; .edu, para universidades; .gov, para el gobierno USA; .mil, para el ejército USA) y los nuevos dominios (.mobi, para páginas específicamente diseñadas para móviles, etc...)

El sistema DNS realiza dos tipos de conversión:

- ☐ Directa: Obtiene la dirección IP de un equipo a partir de su nombre completo.
- ☐ Inversa: Obtiene el nombre completo a partir de su dirección IP.

En el sistema DNS, cada entidad responsable de un dominio lleva la gestión de los dominios o equipos que están por debajo de ese dominio. Por ejemplo, Red.es –que es la entidad responsable de los dominios .es -, se encarga de proporcionar información de donde están los servidores DNS de los dominios ine.es, rtve.es, aeat.es, etc.

1.4 Servicios de Internet

Como hemos comentado antes, Internet se forma porque existen ordenadores que están proporcionando unos servicios (es decir, actúan como servidores) que son consumidos por los equipos clientes.

Estos servicios han ido evolucionando a lo largo del tiempo, pero podemos clasificarlos en los varios tipos:

- ☐ Protocolos de mensajería. En estos protocolos, el usuario redacta un mensaje en el programa cliente y lo envía, bien directamente al otro cliente en base a la información de direccionamiento del servidor, bien lo envía a un servidor (o conjunto de servidores) para que este termine entregándolo al cliente final.
 - Mensajería instantánea (Chat, WhatsApp,...)
 - Mensajería asíncrona (Correo electrónico)
- ☐ Intercambio de ficheros. En este caso, el programa cliente permite transferir ficheros desde un equipo a (o desde) un servidor. Existen varios tipos de protocolos pero el más habitual es FTP
- ☐ Acceso remoto a un servidor. En este caso, desde un programa cliente se accede a controlar otro ordenador (que actúa como servidor). En ocasiones, se utiliza un servidor intermedio que contiene herramientas necesarias para el control. Además de los protocolos tradicionales como SSH, Escritorio Remoto (RDP) o VNC, han aparecido nuevos protocolos como TeamViewer, que, pese a ser muy efectivos, pueden dar lugar a compromisos de confidencialidad.
- ☐ Publicación de información (y, en su caso, interacción) El más conocido es el World Wide Web –en realidad, el protocolo se llama HTTP) y la versión segura (HTTPS)
- ☐ Otros servicios: Base de Datos, directorios LDAP, etc...



1.5 La web

En el comienzo de los años 90, Tim Berners-Lee, uno de los científicos del Laboratorio del CERN (Centro Europeo de Investigación Nuclear) se vio en la necesidad de poder, por un lado, publicar los artículos científicos de manera que fuera cómoda su recuperación y posterior lectura y, por otro lado, poder referirse al documento desde otros documentos.

Para ello, diseñó los siguientes protocolos:

- ☐ URL, que permite referenciar un texto en base al nombre de la máquina y un camino “virtual” hasta el documento
- ☐ HTML, que permite presentar el texto con algunas opciones de resaltado de la información (como subrayados o negrita) y describir, dentro del documento, los enlaces a otros documentos.
- ☐ HTTP, que es el protocolo por el que el servidor que aloja los documentos se comunica con los programas cliente, denominados navegadores.

1.6 Los navegadores

Como ya hemos explicado, Tim Berners-Lee diseñó un “ecosistema” completo que permitiese la consulta rápida de información en línea. Para ello, elaboró también un programa cliente o navegador, denominado WorldWideWeb, que pronto red denominó Nexus para evitar confusiones entre el concepto y el propio software.

Este primer programa tenía funcionalidades que actualmente parecen limitadas, pero ya poseía un interfaz gráfico, así como un editor de páginas HTML embebido. En términos generales, un navegador consiste en un programa software que, a partir de una URL inicial, recupera la página HTML que reside (o que es generada dinámicamente) tras esa URL, interpreta dicha página identificando los recursos a descargar (imágenes, audio, video, etc.) y realiza todas las peticiones al servidor para que le entregue dichos recursos, componiendo la imagen final que presenta al usuario.

A lo largo del tiempo, entre 1991, fecha de aparición de la World Wide Web y, la actualidad, ha habido un gran número de navegadores, muchos de ellos basados en software libre (es decir, de fuentes abiertas), aunque no todos ellos implementan los estándares en la misma medida, habiéndose separado alguno de ellos notablemente de los estándares como Internet Explorer (de Microsoft).

1.7 Buscadores

En un momento inicial, el número de servidores Web existentes era muy reducido, lo que hacía relativamente fácil conocer las URL. En muchos casos, figuraba en los documentos en papel de las investigaciones o en los resúmenes de las mismas.

Sin embargo, en muy poco tiempo, el número de servidores creció exponencialmente. Así, en junio de 1991 había solo uno (el del CERN), y fue creciendo un orden de magnitud cada año, alcanzando los más de 25.000 en 1995 (fecha de puesta en marcha del servidor www.ine.es). Se hizo preciso contar con una herramienta que permitiera localizar las páginas deseadas, para lo cual surgieron los buscadores.

Para obtener la información para el funcionamiento del buscador, un programa, conocido como spider (araña) o crawler (tractor), recorre todas las páginas registradas. Estos, inicialmente, eran de

dos tipos:

- ☐ Mediante clasificación temática realizada o supervisada por personas. En este grupo cabría encuadrar a buscadores como Yahoo (que fue uno de los pioneros y uno de los más usados en los años 90). Los temas para la clasificación se extraían de las etiquetas que figuran en la propia página HTML y se incorporaban al directorio o directorios correspondientes. En este caso, si se buscaba “Estadística” aparecería la parte del directorio de páginas en las que se mencionase la palabra “estadística” en la clasificación temática. Yahoo, como tal buscador basado en directorio, desapareció en 2003. La razón del abandono fue que, desde 1996, la World Wide Web fue creciendo un orden de magnitud cada tres años aproximadamente, llegando a 1.630 millones de sitios web en 2018, haciendo impracticable la supervisión humana.
- ☐ Mediante la búsqueda en el contenido de las páginas después de haber eliminado las palabras “huecas” (se entiende por palabras huecas o vacías los artículos, preposiciones, pronombres, etc., que, en general, aportan muy poca información). Uno de los primeros en utilizar este tipo de modelo fue el buscador Altavista, que finalmente fue adquirido por Yahoo y fusionado con la información de Yahoo, abandonando la búsqueda basada en directorios.


Finalmente, en 1996, Serguéi Brin y Larry Page crearon un buscador que, además de permitir búsquedas en todo el texto del documento –como Altavista- utilizaba el número de enlaces existentes desde otras páginas hacia la analizada como un indicador de “autoridad”. Así, si la página del INE (www.ine.es) se cita en multitud de páginas, saldrá mejor posicionada en el buscador que si apenas tiene enlaces.

1.8 Comunicación a través de internet. Telefonía IP. Videoconferencia

Como ya se ha comentado, una buena parte de los servicios existentes en Internet son servicios que facilitan la comunicación inter-personal. Algunos son unidireccionales, mientras que la mayor parte de ellos permiten la interacción de dos o más personas.

Podemos identificar los siguientes medios de comunicación en Internet:

- ☐ Redes sociales: Permiten expresar una idea, difundir un video, etc... y a través de las opciones de “Me gusta”, “Compartir”, etc... propagar dicha información al resto de la comunidad, que a su vez, pueden participar de la misma manera. Podemos incluir en este grupo Facebook, Twitter, Instagram, etc.
- ☐ Mensajería instantánea: Permite enviar un mensaje instantáneo de un usuario a otro sin esperas. Podemos incluir aquí los distintos Messenger (Yahoo, Facebook, Microsoft) o Whatsapp.
- ☐ Correo electrónico: Permite el envío de mensajes de texto y ficheros asociados entre dos o más personas (emisor y destinatarios). A diferencia de la mensajería instantánea que es síncrona (el emisor lanza el mensaje y es recibido de forma prácticamente instantánea por los destinatarios), el correo electrónico es asíncrono (es decir, el emisor envía el mensaje y este llega al destinatario, pero no necesariamente en una franja temporal concreta, puesto que los servidores de correo pueden almacenar varios mensajes y enviarlos por lotes en el tiempo). Los más conocidos son Gmail y Outlook.com
- ☐ Foros: Muy reemplazados por las redes sociales, los foros son un instrumento de discusión y participación sobre temas especializados, generalmente gestionados por un moderador, en el que un usuario puede crear nuevos hilos de discusión y participación o responder en hilos ya creados.
- ☐ Blogs: Un blog es una página Web asociada a una fecha que pretende emular los registros de bitácora de los marinos o los diarios de memorias, en los que se van publicando entradas periódicamente.

- 
- ☐ Videoconferencia, comunicación (como mínimo bidireccional) simultánea de audio y vídeo entre dos o más personas. Podemos diferenciar varios tipos:
 - Videoconferencias Web o “Webconference”. Se basan en la utilización de un programa concreto (Microsoft Teams, Google Hangout, Cisco Webex, etc.) -que debe ser el mismo por ambas partes- y en el que se debe contar con una “sala” – dedicada / privada o no- en la que los distintos participantes pueden escuchar y ver al resto de participantes y, en ocasiones, compartir ficheros. Como ventajas, estas conferencias web tienen el bajo coste de las mismas, mientras que existe un gran problema de interoperabilidad entre aplicativos ya que no son compatibles entre sí.
 - Videoteléfonos. Cada vez menos frecuentes, podemos encontrar teléfonos fijos que cuentan con pantalla y micrófono que permiten el establecimiento de video-llamadas entre dos personas. También podemos encontrar operadores móviles que permitan video-llamadas dentro de su red.
 - Videoconferencia inmersiva: Aquella en la que por las grandes dimensiones de las pantallas y la calidad tanto de la imagen como del sonido, el usuario deja de percibir la videoconferencia y tiene la sensación de estar físicamente reunido.

2. LA ADMINISTRACIÓN ELECTRÓNICA

Ya en 1992, la entonces Ley de Régimen Jurídico y Procedimiento Administrativo Común – LRJPAC- establecía la posibilidad de establecer tratamientos automatizados que agilizaran la tramitación de expedientes administrativos con características homogéneas.

Posteriormente, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, estableció las características de dichos instrumentos.

Finalmente, la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, estableció el marco específico de la tramitación electrónica de procedimientos administrativos y de servicios, y creó una serie de derechos de los administrados:

- ☐ Derecho a obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos de manera telemática.
- ☐ Derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas.
- ☐ Derecho a conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones.
- ☐ Derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.
- ☐ Derecho a la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.
- ☐ Derecho a obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.
- ☐ Derecho a la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.
- ☐ Ejercer, también en el ámbito del acceso electrónico, los derechos incluidos en el artículo 35 de la Ley de Procedimiento Administrativo vigente entonces:

- Identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos.
- Utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma.
- El acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Constitución y en ésta u otras Leyes.

Si bien fue un paso adelante de gran importancia, se planteaba como una situación “de mínimos”. En ella, solo se exigía que aquello que el usuario veía (el “front-office”, que se podría traducir como los “servicios de ventanilla”) fuese tramitado en formato electrónico, pero no la tramitación interna.

El siguiente paso vino de la mano de las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en las que el acceso electrónico ya no es algo a añadir al procedimiento administrativo, sino que toda la tramitación –administrativa o no- debe ser realizado de manera íntegramente electrónica. De la misma manera, los documentos administrativos pasaran a emitirse en formato electrónico preferentemente, y las notificaciones administrativas pasaran a efectuarse por medios electrónicos de manera preferente.

2.1 Firma electrónica y certificados digitales

Una de las fases fundamentales del procedimiento administrativo estriba en la plena identificación del ciudadano dentro del procedimiento, así como la firma tanto del ciudadano como del propio órgano administrativo o su representante o titular.

En un primer momento, se traspuso la Directiva 1999/93/CE mediante la Ley 59/2003 que definía, en su artículo 3.1, la firma electrónica como “*el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*”

Además, dicha ley distinguía dos tipos de firmas:

- ☐ Firma electrónica avanzada: Art. 3.2) “*La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*”
- ☐ Firma electrónica reconocida: Art. 3.3) “*Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*”

Posteriormente, la firma electrónica fue regulada directamente a nivel europeo, mediante el **Reglamento (UE) 910/2014**. Este establece:

Artículo 25 Efectos jurídicos de las firmas electrónicas

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

Artículo 26 Requisitos para firmas electrónicas avanzadas

Una firma electrónica avanzada cumplirá los requisitos siguientes:



- a) *estar vinculada al firmante de manera única;*
- b) *permitir la identificación del firmante;*
- c) *haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y*
- d) *estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.*

¿Pero, qué es un certificado?

- ☐ Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación (que puede ser una administración o una entidad privada) que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Desde un punto de vista técnico es un conjunto de un par de ficheros (o, en ocasiones, en un fichero contenedor) que contienen las dos parejas de claves generadas en un proceso de generación de claves asimétricas (claves pública y privada). El fichero que contiene la clave pública, firmada electrónicamente por el Prestador de Servicios de Certificación es lo que se denomina “Certificado electrónico”.
- ☐ El certificado, por tanto, da la seguridad de que el prestador confirma que alguien es quien dice ser, y que por lo tanto, que la firma corresponde a esa persona.
- ☐ Hay que destacar que además de certificados correspondientes a personas físicas, también pueden existir certificados de organismos, “**sellos de órgano**”, que identifican y permiten que estos firmen directamente, especialmente importantes en el caso de la tramitación automatizada,

¿Qué formatos de firma existen?


- ☐ Una firma electrónica es un fichero que contiene información sobre el documento original, el firmante, la fecha de la firma, algoritmos utilizados y posible caducidad de la firma y, en ocasiones, el propio documento firmado. Podemos encontrarnos con que el fichero de firma contenga el propio documento sin firmar (firma embebida) o que se encuentre en un fichero separado, con referencias en el fichero de firma.

¿Cómo puedo firmar documentos?

- ☐ La Administración General del Estado ha elaborado dos instrumentos que permiten la firma de documentos:
 - Por un lado, los denominados “Portafirmas” en los que se encuentran, rememorando una bandeja de correo electrónico, los “mensajes” conteniendo los archivos a firmar.
 - De otro lado, las aplicaciones de escritorio de firma (como **Autofirma**), que permiten seleccionar tanto el fichero a firmar como el certificado a firmar

¿Cómo puedo validar certificados o documentos firmados por otros?

- ☐ Para realizar estas tareas y dada la libertad de establecimiento de Prestadores de Servicios de Confianza Cualificados (nueva definición europea de los Prestadores de Servicios de Certificados), la Administración General del Estado ha elaborado dos instrumentos: **@firma** y **VALIDe**
 - @firma es una plataforma que valida un certificado emitido por cualquiera de los prestadores de servicios de certificación admitidos por el Ministerio de Economía y Empresa.

- 
- Al ser este un servicio orientado a las administraciones, se ha diseñado un segundo servicio, VALIDe, en el que se puede, por un ciudadano, validar tanto un certificado como un documento firmado en cualquiera de los formatos admitidos.

2.2 El DNI electrónico

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía del Ministerio del Interior, es el documento que acredita, desde hace más de 70 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

Con motivo de la Ley 59/2003, de firma electrónica, y la necesidad de acreditar, con total garantías, la identidad de una persona y firmar documentos electrónicos con un dispositivo seguro de creación de firma, se consideró que el DNI podía ser la base con la que la Administración podía ofrecer esta acreditación a los ciudadanos.

Por ello, en 2006 se creó el Documento Nacional de Identidad electrónico (DNLe), que incorpora un pequeño circuito integrado (chip), capaz de generar un par de claves (pública y privada) y guardar de forma segura el certificado.

A pesar de la extensión del uso del DNI, su uso como dispositivo de identificación electrónica se ha visto lastrado por la necesidad de contar con un lector.

Para superar esta restricción, en enero de 2015 se estableció el DNI electrónico 3.0, en el que se incorporó una tecnología dual que, además del chip ya existente, permitía la conexión del DNLe mediante la tecnología NFC existente en los dispositivos móviles de última generación, lo que elimina la necesidad de un lector de tarjetas, drivers, etc. facilitando la conexión online y la autenticación del ciudadano.