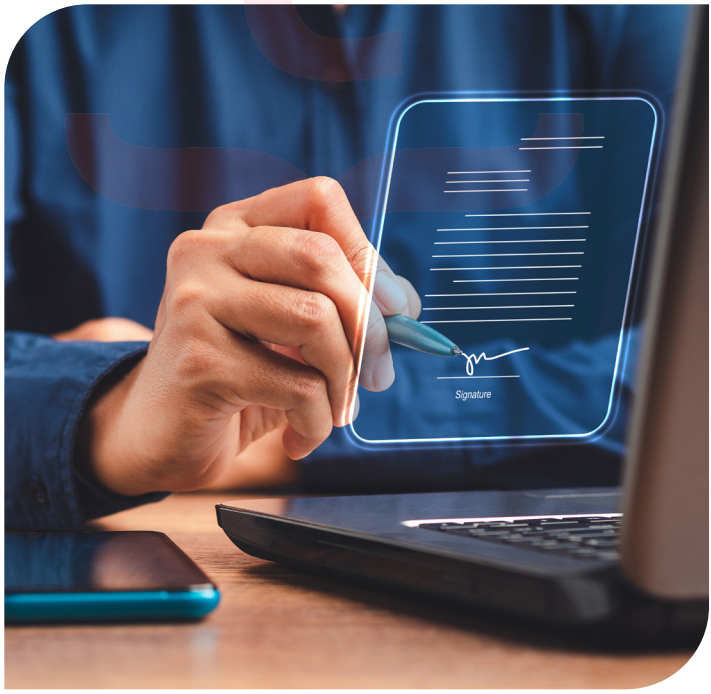
Tema 1

Firma digital. Certificado digital



- Las Tecnologías de la Información y la Comunicación
- La identificación electrónica
- Ley 59/2003 de firma electrónica
- La firma electrónica
- El certificado electrónico
- Tipos de certificado electrónico
- El DNI electrónico
- Aspecto del DNI electrónico
- Usos y ventajas del DNI electrónico

OBJETIVOS:

- Entender los conceptos de identidad y autenticación en el ámbito digital.
- Conocer los distintos tipos de identificación electrónica.
- Familiarizarse con la legislación española sobre firma electrónica.
- Comprender la importancia de esta ley para el desarrollo de la identificación electrónica en España.
- Entender qué es la firma electrónica y cuál es su función en el ámbito digital.
- Conocer los diferentes tipos de firma electrónica.
- Comprender qué es el certificado electrónico y cómo funciona.
- Conocer los diferentes tipos de certificado electrónico.
- Conocer las distintas clasificaciones de los certificados electrónicos.
- Entender qué es el DNI electrónico y cuál es su función.
- Conocer los usos y ventajas del DNI electrónico.

1. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, se refieren a un conjunto de herramientas, técnicas y recursos utilizados para procesar, almacenar, recuperar y transmitir información de manera electrónica. Las TIC son un componente clave en la sociedad moderna, ya que permiten la comunicación instantánea y la transferencia de datos a nivel global. A medida que las tecnologías han avanzado, las TIC se han vuelto cada vez más poderosas y omnipresentes, transformando la forma en que interactuamos y trabajamos.

Las TIC han sido impulsadas por la innovación tecnológica y la creciente demanda de comunicaciones instantáneas, trabajo remoto y acceso a la información en tiempo real. Los dispositivos de comunicación, como los teléfonos móviles, las tabletas y las computadoras, se han vuelto cada vez más sofisticados y accesibles para la mayoría de las personas, lo que ha llevado a un aumento en la adopción de las TIC en todo el mundo.

En la actualidad, las TIC se utilizan en una amplia variedad de industrias y campos, incluyendo la educación, la salud, la banca, el comercio, la industria, la política y la ciencia. Las TIC han transformado la forma en la que se realiza el trabajo y se interactúa, mejorando la eficiencia y reduciendo el tiempo y los costos asociados con la comunicación y el intercambio de información.

Una de las áreas más importantes de las TIC es la **informática**, que incluye el desarrollo de software, el diseño de hardware y la gestión de redes. Los avances en informática han permitido la creación de sistemas más eficientes y confiables, lo que ha llevado a una mayor automatización y ahorro de costos en muchos sectores.

Otro campo de las TIC es la comunicación, que incluye la **transmisión de datos y la conectividad.** Los avances en las comunicaciones han permitido la creación de redes de alta velocidad y la conectividad global, lo que ha mejorado la capacidad de las personas para comunicarse y trabajar juntas a distancia.

La seguridad también es una cuestión importante en las TIC. A medida que la información se ha hecho más accesible y se transmite a través de redes públicas, es más importante garantizar la privacidad y la protección de los datos. Los sistemas de seguridad y cifrado han sido desarrollados para proteger la información y garantizar que solo las personas autorizadas tengan acceso a ella.

Una de las tecnologías clave en la protección de la información es la **firma digital y el certificado digital**. La **firma digital** es una forma de autenticar y validar la identidad de una persona en línea. Al igual que la firma física en un documento, la firma digital permite que una persona firme electrónicamente un documento o un mensaje, garantizando que la información no haya sido alterada y que la persona que lo firmó es la misma que se presentó.

El **certificado digital** es un documento electrónico que se utiliza para verificar la identidad de una persona o entidad en línea. Los certificados digitales son emitidos por autoridades de certificación confiables y se utilizan para garantizar que la información sea segura y privada. Los certificados digitales se utilizan comúnmente en transacciones en línea, como compras en línea y transacciones bancarias.

2. LA IDENTIFICACIÓN ELECTRÓNICA

La identificación electrónica es una forma de autenticación que se utiliza para **verificar la identidad** de una persona en línea. La identificación electrónica se utiliza en transacciones en línea, servicios gubernamentales en línea y otros servicios que requieren la identificación del usuario.

La identificación electrónica se basa en la autenticación y verificación de la identidad del usuario mediante el uso de credenciales electrónicas, como nombres de usuario y contraseñas, certificados digitales o dispositivos de seguridad, como tokens de seguridad o tarjetas inteligentes. Estas credenciales se utilizan para verificar que el usuario que accede a un servicio o sistema en línea es realmente quien dice ser.

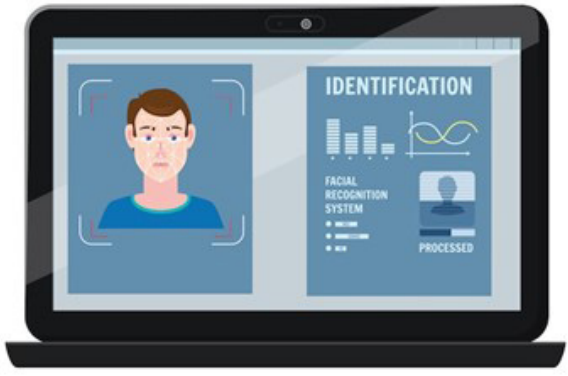
Uno de los métodos más comunes de identificación electrónica es el uso de **nombres de usuario y contraseñas.** Los usuarios crean un

nombre de usuario y una contraseña que utilizan para acceder a un servicio en línea. Sin embargo, este método no es completamente seguro, ya que las contraseñas pueden ser hackeadas o robadas.

Otro método de identificación electrónica es el uso de certificados digitales. Los certificados digitales, como ya se ha indicado, son documentos electrónicos que se utilizan para verificar la identidad de una persona o entidad en línea. Los certificados digitales son emitidos por autoridades de certificación confiables y se utilizan para garantizar que la información sea segura y privada.

Los **dispositivos de seguridad** también se utilizan para la identificación electrónica. Los *tokens* de seguridad y las tarjetas inteligentes son dispositivos que se utilizan para generar contraseñas de un solo uso o códigos de acceso que se utilizan para autenticar la identidad del usuario.

La identificación electrónica es importante porque permite que los usuarios accedan a servicios en línea de manera segura y protege su información personal. Sin embargo, es importante tener en cuenta que **ninguna forma de identificación electrónica es completamente segura.** Los usuarios deben tomar medidas adicionales para proteger su información personal, como utilizar contraseñas seguras y actualizar regularmente sus credenciales de identificación electrónica.



Identificación electrónica

En definitiva, la identificación electrónica es una forma de autenticación que se utiliza para verificar la identidad de una persona en línea. Se basa en el uso de credenciales electrónicas, como nombres de usuario y contraseñas, certificados digitales o dispositivos de seguridad, como tokens de seguridad o tarjetas inteligentes. La identificación electrónica es importante para proteger la información personal de los usuarios; pero es importante tener en cuenta que ninguna forma de identificación electrónica es totalmente segura.

3. LEY 59/2003 DE FIRMA ELECTRÓNICA (DEROGADA, DESARROLLO DE LA LEY 6/2020, DE 11 DE NOVIEMBRE, REGULADORA DE DETERMINADOS ASPECTOS DE LOS SERVICIOS ELECTRÓNICOS DE CONFIANZA)

Importante

Téngase en cuenta que Ley 59/2003, de 19 de diciembre, de firma electrónica, la cual viene incluida en el programa del curso, ha sido derogada con efectos de 13 de noviembre de 2020, por la disposición derogatoria a) de la Ley 6/2020, de 11 de noviembre. Por lo que el presente epígrafe desarrolla la ley vigente.

La Ley 6/2020, de 11 de noviembre, accesible en el siguiente BIDI, es una normativa española que tiene como objetivo regular los servicios electrónicos de confianza, en particular, los relacionados con la firma electrónica, el sello electrónico y el tiempo electrónico. Esta ley pretende garantizar la seguridad y la confianza en las transacciones electrónicas y promover el uso de estos servicios en España.

Ley 6-2020

La Ley 6/2020 establece una serie de definiciones y principios generales para los servicios electrónicos de confianza. En particular, la ley establece que los servicios electrónicos de confianza deben cumplir con los requisitos de seguridad y privacidad necesarios para garantizar la autenticidad, integridad y disponibilidad de los datos y documentos electrónicos. Además, la ley fija que estos servicios deben ser accesibles y utilizables de manera sencilla y eficiente para los usuarios.

En cuanto a la firma electrónica, la Ley 6/2020 establece que se deben utilizar sistemas de firma electrónica avanzada o reconocida para garantizar su validez legal. Además, la ley señala que los prestadores de servicios de certificación deben cumplir con los requisitos y estándares de seguridad necesarios para garantizar la fiabilidad de los certificados electrónicos.

Por otro lado, la ley también regula el uso del sello electrónico, que es un mecanismo de seguridad utilizado para garantizar la autenticidad e integridad de los documentos electrónicos emitidos por organizaciones. La ley establece los requisitos necesarios para utilizar el sello electrónico y los procedimientos necesarios para su emisión y revocación.

Además, la Ley 6/2020 regula el uso del tiempo electrónico, que es un mecanismo utilizado para asegurar la integridad temporal de los documentos electrónicos y su relación con los hechos que documentan. La ley establece los requisitos necesarios para utilizar el tiempo electrónico y los procedimientos necesarios para su emisión y validación.

La Ley 6/2020 de servicios electrónicos de confianza es, por tanto, una normativa importante para el desarrollo de las transacciones electrónicas en España, ya que establece los requisitos y estándares necesarios para garantizar la seguridad y confianza de estos servicios. Esta ley ha contribuido a la adopción de los servicios electrónicos de confianza en España y ha permitido la simplificación y agilización de los procesos administrativos y empresariales en línea.

4. LA FIRMA ELECTRÓNICA

La **firma electrónica** es un mecanismo que permite verificar la autenticidad e integridad de los documentos electrónicos y garantizar su validez legal. La firma electrónica se ha convertido en una herramienta clave para el desarrollo de las transacciones electrónicas en todo el mundo, ya que permite que estas se realicen de manera segura y eficiente.

En términos generales, la firma electrónica es un proceso mediante el cual se asocia una persona, entidad o sistema informático a un documento electrónico, de forma que se pueda comprobar su autoría y la integridad del documento. Para ello, se utilizan tecnologías de criptografía y certificación digital que permiten crear una firma electrónica que cumpla con los requisitos legales y técnicos para su validez.

Existen diferentes tipos de firma electrónica, que varían según su nivel de seguridad y confianza. A continuación, se describen los principales:

- **Firma electrónica simple.** Es una firma electrónica que utiliza una clave privada del firmante para verificar su identidad. Este tipo de firma electrónica es el más básico y tiene un nivel de seguridad bajo.
- **Firma electrónica avanzada.** Es una firma electrónica que utiliza una clave privada del firmante y está vinculada de forma única al firmante. Este tipo de firma electrónica es más segura que la firma electrónica simple y cumple con los requisitos legales para su validez.
- **Firma electrónica cualificada.** Es una firma electrónica avanzada que está vinculada a la identidad del firmante de forma fehaciente y es emitida por un prestador de servicios de certificación acreditado. Este tipo de firma electrónica tiene un nivel de seguridad muy alto y es considerada una prueba legalmente válida de la identidad del firmante.

En España, la firma electrónica estaba regulada por la Ley 59/2003 de Firma Electrónica, que establecía los requisitos y estándares necesarios para la utilización de la firma electrónica en las transacciones electrónicas. La Ley 6/2020 de servicios electrónicos de confianza

ha actualizado y mejorado la regulación de la firma electrónica y otros servicios electrónicos de confianza, tal y como hemos visto en el apartado anterior.

La firma electrónica ha demostrado ser una herramienta muy útil en la gestión de los procesos y transacciones electrónicas, ya que permite garantizar la autenticidad, integridad y confidencialidad de los documentos electrónicos. Además, su uso favorece la agilización y simplificación de los procesos administrativos y empresariales en línea, lo que ha contribuido al desarrollo de la economía digital en todo el mundo.

5. EL CERTIFICADO ELECTRÓNICO

El **certificado electrónico** es un documento digital que vincula una identidad a una clave pública. Esta vinculación es realizada por una autoridad de certificación, que es una entidad confiable que emite y gestiona los certificados electrónicos. El certificado electrónico se utiliza para identificar y autenticar a las personas, empresas u organizaciones en las transacciones electrónicas y garantizar la seguridad y confidencialidad de los datos transmitidos.

El certificado electrónico contiene información sobre la identidad del titular, su clave pública y la información de la autoridad de certificación que emitió el certificado. La información del certificado se almacena en un archivo digital que se puede almacenar en un dispositivo seguro, como una tarjeta inteligente o un token USB. Este archivo digital se utiliza para verificar la identidad del titular en las transacciones electrónicas y garantizar la seguridad de la información transmitida.

Los certificados electrónicos se utilizan para una amplia gama de **transacciones electrónicas,** incluyendo la firma electrónica de documentos, la autenticación en servicios en línea y la encriptación de comunicaciones en línea. En muchos casos, el certificado electrónico es un requisito legal para la realización de determinadas transacciones electrónicas.

En España, la emisión y gestión de los certificados electrónicos está regulada por la Ley 6/2020 de servicios electrónicos de confianza. Esta ley indica, en su Título II, los requisitos y estándares necesarios para la emisión y gestión de los certificados electrónicos y establece la figura del prestador de servicios de certificación como entidad responsable de la emisión y gestión de los certificados electrónicos.

Los prestadores de servicios de certificación son entidades confiables que se encargan de emitir y gestionar los certificados electrónicos. Estas entidades deben cumplir con los requisitos técnicos y de seguridad establecidos por la ley y deben estar acreditadas por el Ministerio de Economía y Empresa para poder operar en España.

El certificado electrónico es una herramienta clave para garantizar la seguridad y confidencialidad de las transacciones electrónicas. Su uso permite la autenticación de las partes involucradas en una transacción electrónica y garantiza la integridad y confidencialidad de los datos transmitidos. Además, favorece la simplificación y agilización de los procesos administrativos y empresariales en línea, lo que ha contribuido al desarrollo de la economía digital en todo el mundo.

6. TIPOS DE CERTIFICADO ELECTRÓNICO

Existen diferentes tipos de clasificación de los certificados electrónicos según el criterio que empleemos para su clasificación.

6.1 Clasificación según el tipo de identidad

- **Certificados de persona física.** Este tipo de certificado es emitido a una persona física y se utiliza para identificar a esa persona en transacciones electrónicas. Este certificado se puede utilizar para firmar digitalmente documentos, contratos y otros tipos de transacciones en línea.
- **Certificados de persona jurídica.** Este tipo de certificado es emitido a una empresa u organización y se utiliza para identificar a esa entidad en transacciones electrónicas. Este certificado se

puede utilizar para firmar digitalmente documentos y transacciones en línea en nombre de la empresa u organización.

- **Certificados de entidad sin personalidad jurídica.** Vinculan a su suscriptor unos datos de verificación de firma y confirma su identidad para ser utilizados únicamente en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario.

6.2 Clasificación según el ámbito de aplicación

Los certificados electrónicos también se pueden clasificar según el ámbito de aplicación en el que se utilizan. A continuación, se describen algunos de los tipos más comunes:

- **Certificado de servidor.** Este tipo de certificado se utiliza para autenticar la identidad de un servidor web y cifrar las comunicaciones entre el servidor y el usuario. Este tipo de certificado es esencial para garantizar la seguridad de las transacciones electrónicas en línea y para proteger la privacidad del usuario.
- **Certificado de pertenencia a empresa.** Este tipo de certificado se emite a los empleados de una empresa para acreditar su pertenencia a la misma y su capacidad para actuar en nombre de la empresa en transacciones electrónicas. Este certificado se utiliza para identificar y autenticar a los empleados de la empresa en transacciones en línea.
- **Certificado de representante.** Este tipo de certificado se emite a una persona para acreditar su capacidad para representar a otra persona o entidad en transacciones electrónicas. Este certificado se utiliza para identificar y autenticar al representante en nombre de la persona o entidad que representa.
- **Certificado de apoderado.** Este tipo de certificado se emite a una persona para acreditar su capacidad para actuar como apoderado de otra persona o entidad en transacciones electrónicas. Este certificado se utiliza para identificar y autenticar al apoderado en nombre de la persona o entidad que representa.
- **Certificado de sello de empresa.** Este tipo de certificado se utiliza para acreditar la identidad de una empresa y su capacidad para emitir facturas electrónicas y otros documentos oficiales.