EUSKAL SINDIKATUA

# TEMA 16

# Legalizaciones de firmas. La validación en la administración electrónica: la identificación y firma electrónica, el certificado electrónico.

# SUMARIO (I)

# SUMARIO (II)

# SUMARIO (III)

| | 1. LEGALIZACIONES DE FIRMAS |
|---|---|
| **Legalizaciones de firmas** | La legalización de firma es un procedimiento distinto de la copia y la certificación: no ratifica la validez del contenido del documento, sino que asegura la identidad de la persona que lo ha firmado.<br>Se realiza insertando en el documento, tras la firma, una diligencia con la fórmula «Diligencia de legalización de firma», seguida de: «De acuerdo con los datos en mi poder, la firma precedente corresponde a [nombre, apellidos y cargo]».<br>Debe llevar, además:<br>– El sello del Departamento u Organismo Autónomo que legaliza la firma.<br>– La fecha de la legalización.<br>– El cargo, nombre y apellidos de la persona que la realiza. |

| | 2. LA VALIDACIÓN EN LA ADMINISTRACIÓN ELECTRÓNICA |
|---|---|
| **Marco normativo general** | La LPACAP y la LRJSP recogieron las disposiciones previas, derogando expresamente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.<br>Matización importante: los apartados sobre el registro electrónico de apoderamientos, registro electrónico, registro de empleados habilitados, punto de acceso general y archivo único electrónico de la derogada Ley 11/2007, de 22 de junio, siguieron vigentes hasta el 2 de abril de 2021 (DF 7.ª LPACAP, prorrogada por la DF 9.ª del derogado RD-ley 28/2020, de 22 de septiembre; y, posteriormente, por la vigente Ley 10/2021, de 9 de julio, de trabajo a distancia).<br>Artículos de especial interés de la LPACAP: art. 6 (registros de apoderamientos); arts. 31 y 32 (cómputo de plazos); arts. 41-43 (notificaciones); art. 53 (derechos del interesado); art. 70 (expediente administrativo). |

**Sistemas de firma para la actuación administrativa**

Regulado en el Capítulo V del Título Preliminar de la LRJSP. El concepto de «firma electrónica» se reserva a las personas físicas, y el de «sello electrónico» a las personas jurídicas.

Art. 42 LRJSP — sistemas de firma para la actuación administrativa automatizada:

- Sello electrónico de AAPP, órgano u organismo, basado en certificado electrónico reconocido o cualificado.
- Código Seguro de Verificación (CSV) vinculado a la AAPP, que permite comprobar la integridad del documento accediendo a la sede electrónica.

Art. 43 LRJSP — la actuación de una AAPP por medios electrónicos se realiza mediante firma electrónica del titular del órgano o empleado público; cada AAPP determina sus sistemas de firma.

Art. 45 LRJSP — para favorecer la interoperabilidad, cuando se usen sistemas de firma distintos del certificado reconocido o cualificado, puede superponerse un sello electrónico basado en certificado reconocido o cualificado al remitir la documentación a otros órganos.

| | 2. LA VALIDACIÓN EN LA ADMINISTRACIÓN ELECTRÓNICA |
|---|---|
| **Marco legal general** | Arts. 40, 41 y 42 LRJSP (identificación, actuación automatizada y sistemas de firma) y art. 43 LRJSP (firma electrónica del personal).<br>ENS, regulado por el RD 311/2022, de 3 de mayo (que derogó el RD 3/2010, de 8 de enero).<br>ENI, regulado por el Real Decreto 4/2010, de 8 de enero.<br>El Reglamento (UE) 910/2014, de 23 de julio (*eIDAS*), relativo a la identificación electrónica y los servicios de confianza, modificado por el Reglamento (UE) 2024/1183 («eIDAS 2»), que introduce la Cartera de Identidad Digital Europea (EUDI Wallet).<br>El RD 203/2021, de 30 de marzo, que aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. |

| | 2. LA VALIDACIÓN EN LA ADMINISTRACIÓN ELECTRÓNICA |
|---|---|
| **Marco legal en la CAE** | El Decreto 91/2023, de 20 de junio, de atención integral y multicanal a la ciudadanía y acceso a los servicios públicos por medios electrónicos, actualmente vigente en la CAE, exige garantizar la autenticidad, integridad, disponibilidad, confidencialidad y conservación de la información y los documentos, fijando el uso de la firma y el certificado electrónicos. (Sustituye al histórico Decreto 232/2007, de 18 de diciembre, derogado por el Decreto 21/2012, de 21 de febrero, y este a su vez por el Decreto 91/2023, de 20 de junio)<br>El Sistema Integral de Gestión Documental de la CAE aplica los principios y requisitos técnicos y legales para el uso fiable de las TIC en cada procedimiento de gestión administrativa, incluidas las validaciones mediante firma electrónica. |

**La firma electrónica: definición**

Estos aspectos estaban regulados en la Ley 59/2003, de 19 de diciembre, de firma electrónica, derogada por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, que desarrolla el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

El art. 3.10 del Reglamento (UE) 910/2014 define 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».

Es una tecnología que protege la información sobre quien consta como signatario, asociando al documento electrónico datos específicos de cada persona que permiten probar el origen y la veracidad de estos.

**Utilización y efectos jurídicos**

La LPACAP concede a la ciudadanía el derecho a utilizar las TIC sin que ello implique restricción alguna al acceso a los servicios públicos.

El Decreto vasco lo plantea de modo inverso, pero equivalente: el uso de medios electrónicos será voluntario y no discriminatorio.

La LPACAP reconoce a la firma electrónica plena validez mediante dos principios:

- Reconocimiento general (no discriminación): el documento electrónico firmado equivale al escrito y firmado en papel a todos los efectos.
- Reconocimiento directo (equivalencia funcional): la firma electrónica puede usarse en todos los casos en que se emplee la firma manuscrita.

**Garantías de la firma electrónica**

Al admitir un documento firmado deben exigirse garantías mínimas, especialmente porque la entrega no suele ser presencial. Toda firma electrónica debe cumplir:

- Identidad: quien firma es realmente quien dice ser.
- Integridad: la información recibida es la remitida en su totalidad y no ha sido manipulada.
- Autenticidad: la información es original y pertenece a quien la emite.
- Irrevocabilidad: quien emite no puede negar haberla remitido, ni que sea la original.
- Confidencialidad: solo emisor y receptor acceden al contenido.

**Firma electrónica, seguridad e interoperabilidad**

El ENS (hoy RD 311/2022, de 3 de mayo, que sustituyó al RD 3/2010, de 8 de enero) considera la firma electrónica no solo como garantía de identidad y de integridad del contenido, sino también como mecanismo de prevención del repudio: quien firma no puede desdecirse después de la información firmada.

El RD 4/2010, de 8 de enero, que regula el ENI, también contempla la firma y los certificados electrónicos; su ámbito sirve de referencia a otras AAPP, favoreciendo el intercambio de datos.

**Tipos de firma electrónica**

La clasificación tradicional (simple/ordinaria, avanzada, reconocida), recogida antes en la Ley 59/2003, de 19 de diciembre, ya no aparece expresamente en la Ley 6/2020, de 11 de noviembre, pero sigue vigente a efectos legales conforme al art. 3 del Reglamento (UE) 910/2014 (que la denomina simple, avanzada y cualificada).

- Ordinaria/simple: la más sencilla; solo identifica al remitente mediante clave de paso, sin garantías sobre el contenido. Uso muy limitado.
- Avanzada: identifica al firmante y la integridad de lo transmitido, bajo su control exclusivo; detecta cambios posteriores, pero no está equiparada a la firma manuscrita sin norma que la habilite.
- Reconocida/cualificada: generada mediante certificado cualificado (tarjeta criptográfica); garantiza plenamente identidad, integridad e irrefutabilidad. Plenamente equiparada a la firma manuscrita, sin necesitar otra legitimación; es la exigida por el ENS para la documentación de nivel medio y alto.

**La firma electrónica en la CAE: condiciones generales**

La firma electrónica en la Administración de la CAE se rige por la LRJSP, la Ley 6/2020, de 11 de noviembre y el Decreto 91/2023, de 20 de junio (que sustituye al histórico Decreto 232/2007, de 18 de diciembre).

Se establece como tipo admitido la firma reconocida/cualificada, tanto para la ciudadanía (personas físicas y jurídicas) como para la propia AAPP, automatizada o no.

Las personas físicas pueden usar también los sistemas de firma del DNI electrónico. Con carácter excepcional, se admiten otros sistemas en: selección y provisión de personal; prestación farmacéutica; cita previa en atención primaria; y otros casos que determine la Vicepresidencia del Gobierno.

**Condiciones adicionales de la firma en la CAE**

Como medida de seguridad añadida, las actuaciones administrativas telemáticas deben incorporar, además de la firma:

- La constancia de que se ha verificado la vigencia de la firma o del certificado electrónico con que se firmó (una firma sin vigencia nunca debe admitirse).
- El sellado de tiempo: acreditación de la fecha y hora de la operación electrónica.

Cualquier cambio en esos datos hace sospechar de una intervención indeseada en el procedimiento o documento, sobre la que habrá que indagar.

**Personas y entes con autorización de firma**

La Administración de la CAE dispone de firma electrónica en tres casos:

- Para el personal a quien competa: cada persona autorizada tiene su propia firma.
- Para el órgano administrativo o puesto directivo: asignada a una persona física, pero utilizable por quien la represente.
- Para la actuación automatizada: la firma la pone el sistema informático sin intervención humana, cuando se comunica un hecho preexistente o se constatan requisitos y se declaran sus consecuencias jurídicas —al no generarse documentación de contenido original, no es necesaria supervisión—.

**El certificado electrónico**

Los arts. 9 y 10 de la LPACAP reconocen el derecho a obtener medios de identificación electrónica.

En la CAE, el Decreto 91/2023, de 20 de junio, establece el uso de certificados electrónicos por la AAPP para validar las firmas de sus órganos y personal, y admite los presentados por la ciudadanía, siempre que estén reconocidos.

El certificado digital es un documento electrónico mediante el cual una autoridad de certificación garantiza la vinculación entre una persona (suscriptor) y su clave pública. Conforme al marco vigente (Ley 6/2020, de 11 de noviembre, y Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014), es el documento firmado electrónicamente por un prestador de servicios de confianza que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

| | |
|---|---|
| **La autoridad de certificación** | Puede ser una persona física o jurídica; en principio, cualquier entidad puede emitir un certificado digital, actuando en libre competencia. A efectos administrativos, debe estar acreditada oficialmente.<br>Funciones: verificar la validez de firmas y certificados; asegurar que los datos del titular son fiables; responsabilizarse legalmente de su calidad y seguridad; registrar a las personas usuarias; y dar sello de fecha y hora de emisión.<br>Entre las autoridades del Estado (registradas en el Ministerio de Asuntos Económicos y Transformación Digital): Agencia Tributaria, CATCert, CERES (FNMT), Izenpe, Dirección General de la Policía, Consejo General de la Abogacía y Colegio de Registradores. |

**Fundamentos técnicos: criptografía asimétrica**

Los certificados electrónicos se basan en métodos criptográficos (criptografía asimétrica), usando un par de claves matemáticamente relacionadas que nunca se repiten:

- Clave privada: sirve para firmar y cifrar el certificado; es única y debe mantenerse en secreto.
- Clave pública: sirve para comprobar y descifrar; está contenida en el certificado y puede ser conocida por cualquiera.

Quien remite el mensaje usa la clave pública para cifrarlo; solo la clave privada da acceso al contenido, garantizando la confidencialidad, y la existencia de la clave privada permite la identificación y autenticación del remitente (salvo robo).

| | |
|---|---|
| **Contenido y utilización del certificado** | Elementos mínimos: nombre y dirección de la autoridad de certificación; número de serie único; fechas de emisión y caducidad; nombre y dirección del titular; su clave pública; y la firma electrónica de la autoridad de certificación.<br>Usos específicos: identificación en portales y aplicaciones; firma y cifrado de documentos y correos; gestiones sanitarias; y trámites administrativos con plenas garantías (contratación, notificaciones, obtención de certificaciones). |

**Tipos de certificado electrónico**

- Personal: la clave privada la posee una persona física, por sí misma o en representación de una persona jurídica.
- De entidad: suscribe y firma una persona jurídica, actuando mediante una persona física poseedora de las claves; vinculado a NIF u organización (CIF).
- De dispositivo: lo utilizan dispositivos o aplicaciones de forma automatizada, sin intervención humana directa ni titular concreto de la clave privada; suele depender de una persona jurídica.

**Ciclo de vida del certificado electrónico**

El certificado no tiene validez indefinida (como máximo, suele ser de cuatro años). Puede encontrarse en cuatro estados:

- Suspensión: invalidación temporal (máximo 120 días naturales); recomendada ante sospecha de pérdida o robo de la clave.
- Habilitación: reactivación de un certificado suspendido, dentro del plazo de suspensión y antes de caducar.
- Revocación: invalidación irreversible, tras suspensión o estando vigente, por voluntad de quien esté autorizado.
- Renovación: solicitud de un nuevo certificado por haber caducado el anterior.

**La certificación electrónica en la CAE**

El Decreto 91/2023, de 20 de junio exige que los certificados electrónicos identifiquen al órgano o puesto directivo competente y a la persona titular. Los del personal identifican a la persona física, la entidad y, en su caso, el puesto de trabajo.

Obligaciones de las personas identificadas en los certificados: custodiar los datos de creación de firma; utilizar el certificado dentro de sus límites; y solicitar su suspensión o revocación si se pone en peligro el secreto de los datos o hay uso indebido por terceros.

Los certificados reconocidos de otras autoridades son admitidos si el prestador facilita la información necesaria, de forma accesible y sin coste; por reciprocidad, también pueden admitirse certificados no reconocidos de otras AAPP.

## 2. LA AUTORIDAD DE CERTIFICACIÓN VASCA: IZENPE

**Izenpe: presentación**

Izenpe, S.A. (Ziurtapen eta Zerbitzu Enpresa) es la entidad vasca prestadora de servicios de certificación electrónica, con sede en Vitoria-Gasteiz. Su creación partió del Gobierno Vasco, con la colaboración de las Diputaciones de Álava, Bizkaia y Gipuzkoa.

Al ser una autoridad de certificación reconocida, las certificaciones que expide tienen plena validez administrativa y legal durante su vigencia.

## 2. LA AUTORIDAD DE CERTIFICACIÓN VASCA: IZENPE

**Izenpe: definición y objetivos**

Izenpe se define como entidad prestadora de servicios de certificación: proporciona servicios de firma y certificado electrónicos.

Objetivos generales:

- Fomentar el gobierno electrónico con garantías de seguridad, confidencialidad, autenticidad e irrevocabilidad.
- Prestar servicios de seguridad, técnicos y administrativos en las comunicaciones de las instituciones públicas vascas.
- Expedir y suministrar certificaciones electrónicas a personas físicas y entidades públicas y privadas.
- Expedir certificaciones de servidor *web* y elementos de *software*, y prestar consultoría.

**Tipos de certificados de Izenpe**

Izenpe expide trece tipos de certificado; los de mayor relación con la labor administrativa son:

- De ciudadano: firma reconocida, para personas físicas mayores de 16 años, vinculado a servicios públicos.
- De entidad (con y sin personalidad jurídica): para organizaciones, o para comunicaciones en el ámbito tributario.
- Corporativo reconocido (público/privado) y de personal de entidades públicas: identifican a personas con cargos en entidades, según ejerzan o no potestades administrativas.
- De órgano administrativo y sello electrónico (para actuación automatizada, validez de tres años).

| | 3. EL USO DE LOS CERTIFICADOS EN LA ADMINISTRACIÓN GENERAL DE LA CAE |
|---|---|
| **Uso de certificados por la ciudadanía** | En el ámbito de la Administración General de la CAE, la Orden de 27 de junio de 2012, de la Consejera de Justicia y Administración Pública, por la que se aprueba la política de firma electrónica y de certificados, aprueba la política de firma electrónica y de certificados (dictada al amparo del art. 19 del Decreto 21/2012, de 21 de febrero; la base legal vigente es hoy el art. 69 del Decreto 91/2023, de 20 de junio).<br>La ciudadanía puede identificarse, entre otros medios, mediante: DNI/NIE con contraseña y coordenadas o código *SMS*; certificado profesional en la nube; o certificados digitales reconocidos. |

**Uso de certificados por empleados públicos vascos**

El personal al servicio de las AAPP vascas puede identificarse mediante:

- Tarjeta Izenpe de empleado/a y *PIN*.
- «Giltza profesional»: certificado en la nube para el personal empleado público, con contraseña y una clave de un solo uso (recibida por SMS o correo electrónico).