

**Reglamento por el que se regula la  
videoconferencia como sistema de identificación y  
firma**

## **Preámbulo**

El Real Decreto 463/2020, de 14 de marzo, por el que se declaró el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 , así como las restantes normas aprobadas a posteriori con el objetivo de evitar la propagación de la pandemia, hicieron muy difícil o imposible la tramitación presencial de procedimientos administrativos por aquellos interesados que, de acuerdo con la actual normativa, no están obligados a interactuar electrónicamente. Es por ello que, desde esta Corporación Insular se ha detectado la necesidad de adoptar medidas que faciliten que estos colectivos puedan interactuar a través de otros canales con la Administración.

En este sentido, el artículo 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), especialmente en su apartado 1, dispone: “Las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen”.

Es necesario, por tanto, en este contexto en el que la atención presencial se ha visto notoriamente afectada y en aras a garantizar el funcionamiento básico de los servicios, instaurar un nuevo canal que permita a los interesados la tramitación de sus procedimientos cuando no se dispone de la tecnología o el conocimiento necesario para poder hacerlo a través de la sede electrónica de esta Corporación. Ahora bien, esta implementación ha de estar acompañada de todas aquellas medidas de seguridad jurídica que garanticen la validez de lo actuado.

A este respecto, La LPACAP en el marco de un procedimiento administrativo establece la obligación de las Administraciones Públicas de verificar la identidad de los interesados, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente, pudiendo éstos hacerlo, entre otros, a través de sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que sólo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

De igual forma, y en lo que atañe a la firma, de acuerdo con lo estipulado en el artículo 11 de la LPACAP, resulta obligatoria la misma en la interacción de la ciudadanía con la Administración, entre otros, para formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones o renunciar a derechos, reafirmando tal obligación su artículo 66 cuando se afirma que las solicitudes que se formulen deberán contener la firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.

Con respecto a los sistemas de firma de los que pueden hacer uso los interesados, la LPACAP en su artículo 10, reconoce que los mismos podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento, considerándose como válido a estos efectos, entre otros, cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, añadiendo en su apartado 4, que las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en la LPACAP como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados

Por otro lado, a la hora de establecer y regular los sistemas de firma ha de tenerse en cuenta lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) que tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad sobre protección de la información, así como, la normativa en materia de protección de datos, esto es, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Pues bien, el Real Decreto en su artículo 33 establece la obligatoriedad de que la Política de Firma concrete los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas. Por otra parte, el RD en su anexo II punto 5.7.4 es muy específico sobre los tipos de firma que deben aplicarse en función del nivel de la información (bajo, medio o alto) que debe protegerse. Por lo que a la hora de establecer sistemas de firmas debe tenerse en cuenta la seguridad de los distintos tipos de firma en función de la mayor o menor sensibilidad de la información que se trate.

En atención a lo expuesto, resulta necesario implementar un sistema de identificación y autenticación que, en aplicación del principio de proporcionalidad, adaptándose a la realidad que se está experimentando como consecuencia de las restricciones a la libertad de movimiento de la ciudadanía, cumpla con todas las garantías jurídicas y de seguridad, de modo que se pueda identificar de forma inequívoca al ciudadano/a que se relaciona con la Administración, al tiempo que, tratándose de presentación de solicitudes, se garantice la **autenticidad de la expresión de su voluntad y consentimiento**, así como la **integridad e inalterabilidad** del documento y su adecuación al ENS.

El presente Reglamento es coherente con los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento

Administrativo Común de las Administraciones Públicas. De lo expuesto en los párrafos anteriores se pone de manifiesto el cumplimiento de los principios de necesidad y eficacia. El Reglamento es acorde al principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados, e igualmente se ajusta al principio de seguridad jurídica. Por último, con respecto al principio de eficiencia, queda garantizado por cuanto se implementa un sistema que si bien puede implicar un aumento de las cargas administrativas, éstas son imprescindibles y en ningún caso innecesarias.

Con todo lo expuesto, se pretende instaurar la videoconferencia como un sistema de identificación y firma en las relaciones con la ciudadanía para determinados procedimientos, siempre con estricto cumplimiento a lo previsto en el actual marco normativo, regulando los términos y condiciones que a continuación se recogen.

## **Título Preliminar. Disposiciones generales**

### **Artículo 1.- Objeto**

El presente Reglamento tiene por objeto la regulación del sistema de videoconferencia como un sistema de identificación y firma, que permita al Cabildo de Tenerife por un lado, verificar la identidad de los interesados en los procedimientos administrativos de su competencia y por otro, permitir acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

Este sistema de identificación y firma se circunscribe a la relación de la ciudadanía con la Administración, en el marco de aquellos procedimientos que sean previamente autorizados por el órgano de gobierno que tenga atribuida la competencia en materia de administración electrónica de las entidades previstas en el ámbito subjetivo del presente documento y que serán publicados, para su general conocimiento, en la sede electrónica de esta Corporación Insular ([www.sede.tenerife.es](http://www.sede.tenerife.es)), teniendo en cuentas los tipos de firma que deben aplicarse en función del nivel de la información que debe protegerse, de acuerdo con lo previsto en el el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, esto es, cuando el sistema de información, o la segmentación correspondiente del mismo, asociado al trámite o procedimiento, haya recibido, según el criterio establecido en el Esquema Nacional de Seguridad, la categoría Básica o Media.

### **Artículo 2.- Ámbito subjetivo de aplicación**

El ámbito subjetivo de aplicación del presente reglamento es el Cabildo de Tenerife, así como sus Organismos Autónomos, Entidades Públicas Empresariales y Consorcios adscritos, de conformidad con lo que, en su caso, acuerden sus órganos competentes, en virtud de su autonomía organizativa y dentro del marco normativo aplicable.

## **Título I. De los interesados en el procedimiento de identificación y firma**

### **Artículo 3.- Sujetos a los que se les aplica el sistema de identificación y firma**

1.- De acuerdo con el artículo 14.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no. En este sentido, el presente Reglamento tiene por destinatarios aquellas personas físicas, no obligadas a relacionarse electrónicamente con el Cabildo, que careciendo de sistemas de identificación y firma electrónica previstos en los apartados a) y b) del artículo 10.2 de la LPACAP, o cualesquiera otros sistema instaurado por esta Administración y autorizado por el Estado al amparo de lo previsto en el artículo 9.2 c) y 10.2 c) de la LPACAP, necesiten relacionarse con el Cabildo de Tenerife sin necesidad de hacerlo presencialmente.

## **Título II. Del procedimiento de identificación y firma**

### **Artículo 4.- Solicitud del servicio**

1. La solicitud para hacer uso de este sistema de identificación y firma para interactuar con la Administración en el marco de un procedimiento administrativo podrá llevarse a cabo por alguno de los siguientes medios:

- Por correo electrónico:

El ciudadano/a enviará un correo a la dirección que se indique por las entidades comprendidas en el ámbito subjetivo del presente Reglamento, para pedir cita a través de videoconferencia, debiendo indicar el procedimiento para el que solicita ser atendido, así como, la actuación que desea realizar con respecto al procedimiento, esto es, presentar una solicitud, una declaración responsable o comunicación, interponer recurso, desistir de acciones o renunciar a derechos o simplemente solicitar información.

Además, se le solicitará una dirección de correo electrónico, a los efectos de entablar las futuras comunicaciones.

- Mediante el envío de formulario web que se pondrá a disposición de la ciudadanía en las sedes electrónicas de las entidades relacionadas en el artículo segundo del presente reglamento.

2. El personal de las oficinas de asistencia en materia de registro, una vez recibida la solicitud, enviará un correo electrónico al interesado/a con las instrucciones para la videoconferencia y la relación de documentación que debe aportar, antes de que tenga lugar la cita.

A tal efecto, la citada relación contendrá los siguientes documentos:

- La solicitud (que incluye la cláusula informativa en materia de tratamiento de datos de carácter personal y la no oposición a la intermediación de datos)
- El listado de documentos que debe aportar, asociados a cada procedimiento.

3. El solicitante (ciudadano/a) debe remitir por correo electrónico la solicitud cumplimentada y la documentación requerida que se indican en el apartado anterior y

la copia (foto o escaneo) del anverso y reverso del documento de identificación, que deberá ser:

3.1 Para las personas físicas de nacionalidad española, el Documento Nacional de Identidad.

3.2 Para las personas físicas de nacionalidad extranjera, la Tarjeta de Residencia, la Tarjeta de Identidad de Extranjero y el Pasaporte o, en su caso, el documento de identidad del país de origen en vigor.

Si el solicitante o interesado es una persona física menor de edad o con falta de capacidad de obrar, se deberá remitir la copia (foto o escaneo) del anverso y reverso del documento identificativo tanto del solicitante o interesado como de su representante.

4. El gestor, funcionario de las Oficinas de Asistencia en materia de Registro, hará las comprobaciones necesarias a la vista de la documentación remitida, antes de establecer la videoconferencia. En caso de que el ciudadano/a no aporte toda la documentación indicada o bien ésta no tenga una calidad suficiente para ser completamente legible, se le informará, a través del correo electrónico, de la documentación que resulta preceptiva para completar la petición de acceso al servicio de videoconferencia. En tal sentido, se entiende que el documento tiene calidad suficiente cuando la digitalización se realiza con una resolución de 200 píxeles por pulgada (ppp). Además, se recomienda un formato de salida tipo PDF, aunque son válidos todos los relacionados por la Norma Técnica de Interoperabilidad (NTI) de Catálogo de Estándares, esto es, documentos pdf, jpeg,png,tiff.

5. Una vez se disponga, conforme exige el trámite, de la documentación requerida, el gestor concretará una cita con el ciudadano/a remitiendo a la dirección del correo electrónico del solicitante la dirección de acceso a la sala de la videoconferencia, fijando la fecha y hora de la misma.

#### **Artículo 5.- Identificación por videoconferencia**

1. El gestor procederá a la carga de la solicitud y documentación presentada por el ciudadano/a en la aplicación del registro e iniciará la videoconferencia en la fecha y la hora establecida y esperará durante un periodo de cortesía de cinco minutos. En caso de que el ciudadano/a no se personase, se le remitirá un correo electrónico indicándole que al no haberse presentado al acto se entiende que desiste de su petición de acceso al servicio de videoconferencia.

2. Personado el ciudadano/a, el gestor le informa que la videollamada será objeto de grabación y a los efectos de dejar evidencias en la verificación de la identidad para la firma, se solicitará la identificación del ciudadano/a, para lo cual el empleado público indicará la fecha y la hora y le solicitará que muestre de forma claramente visible el documento identificativo por ambas caras e indique su nombre y apellidos y su NIF/NIE, procediendo a su cotejo con el remitido por el ciudadano/a a través de correo electrónico. En el caso de que concuerden se continuará con el proceso.

3. En el supuesto de que los solicitantes o interesados fueren personas físicas menores de edad o con falta de capacidad de obrar, se procederá a la identificación tanto del menor o la persona incapacitada como de la persona que ejerce la patria potestad o tutela judicial efectiva. En este sentido, se procederá conforme a lo señalado en el apartado anterior.

4. En caso de que las condiciones de la transmisión impidan o dificulten verificar el proceso se estará a lo previsto en el apartado décimo del presente reglamento relativo a la gestión de incidencias.

#### **Artículo 6.- Gestión del procedimiento para la autenticación y presentación**

1. Realizado con éxito el proceso de identificación, y a fin de verificar por parte del interesado/a los datos a firmar, mostrará por pantalla y expondrá a viva voz el contenido de la solicitud y relacionará el resto de la documentación remitida para el trámite.

Con la finalidad de dejar evidencia del consentimiento explícito del/a interesado/a con el contenido a firmar, en el mismo acto, el gestor recabará del ciudadano/a su manifestación de consentimiento y expresión de su voluntad de firmar, para lo cual se le pedirá que confirme expresamente si son ciertos los datos a firmar y muestre su conformidad con el contenido de los documentos que aportó a través de correo electrónico y las declaraciones que realiza en el acto y que se relacionan a continuación, dejando constancia expresa de su voluntad en la grabación de la videoconferencia:

- La solicitud (que incluye la cláusula informativa en materia de tratamiento de datos de carácter personal y la no oposición a la intermediación de datos) con la documentación aportada.
- Declaración sobre su consentimiento al empleo del sistema de videoconferencia como medio de identificación y autenticación de su declaración de voluntad.
- La declaración responsable en la que manifieste la no disponibilidad de medios electrónicos para la identificación y firma a través de sistemas regulados en los apartados a) y b) de los artículos 9 y 10 de la LPACAP o cualesquiera otros sistema instaurado por esta Administración y autorizado por el Estado al amparo de lo previsto en el artículo 9.2 c) y 10.2 c) de la LPACAP, así como, la veracidad de los documentos que presenta.

2. Seguidamente el gestor procederá a su registro en la aplicación del Registro Electrónico General – Geiser. La integridad y conservación de los datos firmados y de las evidencias de la firma se garantizará con las medidas previstas en el apartado cuarto del artículo noveno del presente reglamento. Una vez realizado el registro del trámite, el gestor remitirá al correo electrónico del solicitante el documento justificativo del registro de entrada de su solicitud junto con la documentación presentada.

3. Sin perjuicio de lo dispuesto en los apartados anteriores, realizado con éxito el proceso de identificación, una vez se disponga de forma efectiva de la figura de los

funcionarios habilitados y se cuente con la regulación pertinente y los sistemas o medios electrónicos necesarios para que pueda actuar conforme a lo previsto en la Ley de Procedimiento, la autenticación de la solicitud y documentación aportado por el ciudadano correspondiente al procedimiento administrativo podrá realizarse a través de la figura del funcionario público habilitado mediante el uso del sistema de firma electrónico del que esté dotado para ello.

#### **Artículo 7.- Remisión al servicio responsable de la tramitación**

El servicio gestor responsable de la tramitación del procedimiento recibirá la solicitud y documentación que la acompaña junto con el fichero de la firma, bien a través del gestor de expedientes corporativo, si el procedimiento se encuentra incluido para su tramitación electrónica, bien a través del Registro electrónico corporativo -GEISER-, en caso contrario.

#### **Artículo 8.- Requisitos para la realización de la videoconferencia**

1. La herramienta de videoconferencia que se empleará deberá disponer de certificación de conformidad con el Esquema Nacional de Seguridad (RD 3/2010) en el nivel Alto, lo que garantiza la privacidad, la seguridad en la transmisión y la autenticidad e integridad de las grabaciones realizadas. De igual forma, la herramienta deberá garantizar que la video-identificación se realiza desde un único dispositivo, que las imágenes y el sonido son inmediatamente transmitidos en formato digital, sin alteración y en directo y que las grabaciones se realizan de forma inmediata, y la misma deberá cumplir con lo indicado en el Reglamento General de Protección de Datos (REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016).
2. Con carácter previo al inicio del funcionamiento del sistema propuesto, se realizará un Análisis de Riesgos según lo indicado en la medida 4.1.1 Análisis de riesgos [op.pl.1] del marco operacional definida en el Esquema Nacional de Seguridad.

#### **Artículo 9.- Grabación, integridad y conservación**

1. La grabación de la conversación que tenga lugar durante el proceso de identificación y autenticación, se realizará en directo (streaming), no admitiéndose ficheros con pregrabaciones y haciendo uso exclusivamente de las herramientas definidas por el Cabildo.
2. El fichero de grabación en vídeo y audio contendrá:
  - Evidencias del consentimiento explícito del/a interesado/a con el contenido firmado.
  - Evidencias para la verificación de la identidad para la firma
3. El fichero con la grabación forma parte del expediente administrativo y se almacenará para su conservación el mismo periodo de tiempo que el establecido para el procedimiento administrativo al que afecta.
4. La integridad y conservación de los datos firmados y de las evidencias de la firma se garantizarán:

- Almacenando el fichero de grabación o de evidencias en un repositorio corporativo de documentos electrónicos, que tenga capacidad de generar un identificador único para el mismo (o URI) que incorpore una función Hash o de resumen, lo que asegura que el mismo no podrá ser modificado sin alterar su identificador.
- Adjuntando, a través de su URI, el fichero de grabación o de evidencias, a la solicitud que se está firmando.
- Aplicando sobre el conjunto, al realizar el registro de la solicitud, un sellado electrónico, con sello electrónico de órgano, al que se añadirá un sello de tiempo emitido por un proveedor cualificado (TSA).
- Una vez realizada la firma, Incorporando toda la información a los sistemas de información corporativos asociado a la tramitación electrónica de procedimientos administrativos, en donde se aplicarán las medidas de seguridad correspondientes del Esquema Nacional de Seguridad.

### **Artículo 10 .- Gestión de incidencias**

Si durante el proceso de celebración de la videoconferencia se apreciara la concurrencia de algunas de las circunstancias que se detallan a continuación, habrá que estar a los efectos en cada caso previsto en este apartado:

#### 1. Durante la videoconferencia

1.1 En el caso de que durante la celebración de la videoconferencia surgieran problemas técnicos que impidan o dificulten la celebración de la misma en las condiciones de seguridad jurídica necesaria para dotar de validez al acto, se reprograma una nueva cita, se cancela la que esté abierta, y se generará una incidencia en el Centro de Atención al Usuario (CAU)

1.2 En caso de cortarse la conversación, el Cabildo repetirá la videollamada y comenzará con el proceso de identificación desde el inicio, antes de continuar con los trámites.

#### 2. Suplantación de identidad

De detectarse un incidente de suplantación de identidad o cualquier otro de naturaleza jurídica, se dará traslado del mismo al órgano insular competente a los efectos legales oportunos.

Y en cuanto a lo que concierne a una incidencia de seguridad informática, se ejecutará el protocolo de incidentes de seguridad, comunicándolo previamente al Delegado de Protección de Datos e informando conforme al protocolo de brechas de seguridad.

#### 3. Uso no adecuado de herramientas:

Si se apreciare el empleo por el personal de la Corporación de un uso inapropiado de las herramientas puestas a disposición para el funcionamiento de este servicio, se seguirá el procedimiento descrito en la Normativa general de uso de servicios TIC del ECIT.

**Disposición adicional primera.- Servicio de información**

No obstante lo previsto en el articulado de este reglamento, cuando el ciudadano/a lo que solicita sea información a través del sistema de videoconferencia, pero referido con carácter general a un trámite, actividad o actuación competencia del Cabildo de Tenerife o de cualesquiera de las entidades previstas en su ámbito subjetivo, para los que no se requiera la identificación y autenticación del ciudadano/a conforme al marco normativo actual, no será de aplicación lo regulado en el Título II del presente reglamento. En estos casos, el ciudadano/a podrá solicitar este servicio de información con videollamada, a través del canal telefónico o mediante correo electrónico, debiendo indicar únicamente un teléfono que permita contactar con el ciudadano para comunicarle la dirección de acceso a la sala de la videoconferencia, fijando la fecha y hora de la misma.

**Disposición adicional segunda.-** Auditoría de seguridad

De acuerdo a lo establecido en el RD 3/2010, específicamente en el artículo 34 y en el Anexo III, se verificará de forma periódica el cumplimiento de los requisitos de seguridad establecidos en los capítulos II y III y en los Anexos I y II del Esquema Nacional de Seguridad, emitiendo el correspondiente informe de auditoría.

**Disposición adicional tercera.-** Formación al personal que gestiona los procesos de identificación y autenticación

Con carácter previo a la puesta en funcionamiento del sistema previsto en el artículo 8 al personal que gestione los procesos de identificación y autenticación por videoconferencia se le impartirá la formación adecuada en el uso y manejo de la herramienta y gestión de las eventuales incidencias.

**Disposición final única.-** Entrada en vigor

El presente reglamento entrará en vigor a partir de la publicación del texto íntegro en el Boletín oficial de la Provincia y haya transcurrido el plazo establecido en el artículo 65.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.