B) Disposiciones y Actos

Junta de Gobierno de la Ciudad de Madrid

3100 *Acuerdo de 18 de noviembre de 2021 de la Junta de Gobierno de la Ciudad de Madrid por el que se aprueba la Política de Identificación y Firma Electrónicas del Ayuntamiento de Madrid y se modifican el Acuerdo de 5 de septiembre de 2019, de organización y competencias de la Coordinación General de la Alcaldía y el Acuerdo de 25 de junio de 2020, por el que se aprueban las Directrices de Técnica Normativa y Administrativa del Ayuntamiento de Madrid.*

La Ordenanza de Atención a la Ciudadanía y Administración Electrónica del Ayuntamiento de Madrid, de 26 de febrero de 2019, establece en su artículo 43.4 que el Ayuntamiento de Madrid aprobará el "Documento de Política de Identificación y Firma Electrónica" al objeto de establecer el conjunto de criterios y las condiciones generales aplicables a la firma electrónica para su validación y su uso en la relación electrónica del Ayuntamiento de Madrid con la ciudadanía, así como entre los órganos y las entidades de aquél con otras Administraciones públicas.

Asimismo, el Plan de Choque de Racionalización y Simplificación de Procedimientos y de Impulso de la Administración Digital, aprobado por Acuerdo de la Junta de Gobierno de 1 de julio de 2021, prevé como una de las medidas de simplificación del acceso electrónico de ciudadanos y empresas la aprobación de un nuevo documento de política de identificación y firma electrónica, en el que se describirá la forma en la que se utilizarán los nuevos sistemas.

Por tanto, en cumplimiento de ambos mandatos, y en el marco de lo establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, resulta necesario que el Ayuntamiento de Madrid apruebe unas directrices relativas a la política de identificación y firma electrónicas.

Para el Ayuntamiento de Madrid resulta fundamental el impulso y la satisfacción de la ciudadanía en el uso de los servicios públicos digitales. Por ello, es prioritario disponer de servicios digitales seguros, sencillos, intuitivos, efectivos y eficientes.

Entre los elementos que sirven al fin anterior se encuentran los sistemas de identificación y firma electrónicas, que garantizan la autenticidad, seguridad e integridad de la relación digital.

En este sentido, para facilitar la realización de trámites y el acceso de la ciudadanía a la información disponible, se establecen en la política de identificación y firma electrónicas cuatro niveles de seguridad. Asociados a estos niveles, se establecen los diversos mecanismos de identificación y firma electrónicas que se admiten en el Ayuntamiento de Madrid, lo que permite graduar su empleo en función del nivel de seguridad más acorde al trámite o a la información de que se trate.

Con el mismo criterio, se establecen también los mecanismos de identificación y firma que el Ayuntamiento de Madrid y sus empleados públicos podrán utilizar en la gestión de procedimientos administrativos, así como en sus relaciones internas.

En definitiva, es un objetivo esencial del Ayuntamiento de Madrid implantar de forma ágil los nuevos mecanismos de identificación y firma electrónicas que la tecnología permita, con la finalidad de reducir la brecha digital y facilitar la comunicación de la ciudadanía. Por tal motivo, la Política de Firma se irá ampliando sucesivamente para incorporar nuevos medios de identificación y de firmas paralelamente a su implantación efectiva.

En su virtud, de conformidad con lo dispuesto en los artículos 17.1 b) y h), y 17.2 de la Ley 22/2006, de 4 de julio, de Capitalidad y de Régimen Especial de Madrid, y en el artículo 19 del

Reglamento Orgánico del Gobierno y de la Administración del Ayuntamiento de Madrid, de 31 de mayo de 2004, a propuesta de la Coordinadora General de la Alcaldía, que eleva la Secretaria de la Junta de Gobierno, y previa deliberación, la Junta de Gobierno de la Ciudad de Madrid, en su reunión de 18 de noviembre de 2021

ACUERDA

PRIMERO.- Aprobar la Política de Identificación y Firma Electrónicas del Ayuntamiento de Madrid que se inserta como anexo.

SEGUNDO.- El sistema de identificación y firma electrónicas previsto en la Resolución de 7 de abril de 2015 del Director General de Calidad y Atención al Ciudadano por la que se aprueban las instrucciones relativas al sistema de identificación basado en clave de usuario y contraseña y a la habilitación del sistema de firma electrónica temporal sin certificado para su utilización en el Registro Electrónico del Ayuntamiento de Madrid, se declara un sistema a extinguir dada su obsolescencia técnica. Por tal motivo, no se admitirán nuevos usuarios en este sistema, ni renovaciones de los existentes, si bien las actuales claves de usuario y contraseña podrán seguir utilizándose hasta que se produzca su caducidad.

TERCERO.- Quedan sin efecto las siguientes disposiciones:

a) Acuerdo de 13 de octubre de 2011 de la Junta de Gobierno de la Ciudad de Madrid, por el que se aprueban los criterios de implantación, organización y uso de la firma electrónica en el Ayuntamiento de Madrid.

b) Decreto de 9 de abril de 2013 de la Delegada del Área de Gobierno de Economía, Hacienda y Administración Pública por el que se aprueba la Instrucción 4/2013, relativa a la implantación de la firma electrónica de empleado público en el Ayuntamiento de Madrid.

Asimismo, quedan sin efecto cuantas disposiciones se opongan, contradigan o resulten incompatibles con lo establecido en el presente acuerdo.

CUARTO.- Modificar del Acuerdo de 5 de septiembre de 2019 de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias de la Coordinación General de la Alcaldía, en los términos que se indican a continuación:

En el apartado 8.º, se modifica la letra i) del punto 1.1, que queda redactada en los siguientes términos:

"i) Definir la política en materia de identificación y firma electrónicas en el Ayuntamiento de Madrid y en sus relaciones con la ciudadanía; planificar y coordinar su implantación y velar por su adecuación a los requerimientos técnicos y a la normativa vigente".

QUINTO.- Modificar las Directrices de Técnica Normativa y Administrativa del Ayuntamiento de Madrid, aprobadas por Acuerdo de 25 de junio de 2020 de la Junta de Gobierno de la Ciudad de Madrid, en los términos que se indican a continuación:

En el apartado 3.º, se añade un último párrafo en el punto 7.4, que queda redactado en los siguientes términos:

"Si se trata de actos que se firmen de forma masiva y automatizada, en la composición de la firma se podrá prescindir de la referencia al cargo, nombre y apellidos del firmante, manteniendo la mención «Firmado electrónicamente», siempre y cuando dicha información se incorpore al acto mediante la firma electrónica".

SEXTO.- La Junta de Gobierno mantendrá permanentemente actualizada la Política de Identificación y Firma Electrónicas del Ayuntamiento de Madrid acordando, en su caso, las modificaciones que estime oportunas. Sin perjuicio de lo anterior, deberá realizarse una revisión de la Política cada 2 años.

SÉPTIMO.- Se faculta al titular de la Coordinación General de la Alcaldía para resolver las dudas que pudieran surgir en la interpretación y aplicación del presente acuerdo.

OCTAVO.- Se faculta al titular de la Dirección General de la Oficina Digital para dictar las resoluciones que sean necesarias para el desarrollo y la ejecución del presente acuerdo.

NOVENO.- El presente acuerdo surtirá efectos desde la fecha de su adopción, sin perjuicio de su publicación en el "Boletín Oficial de la Comunidad de Madrid" y en el "Boletín Oficial del Ayuntamiento de Madrid".

DÉCIMO.- Del presente acuerdo se dará cuenta al Pleno, a fin de que quede enterado, así como a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

Madrid, a 18 de noviembre de 2021.- La Directora de la Oficina del Secretario de la Junta de Gobierno, Carmen Toscano Ramiro.

ANEXO

POLÍTICA DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICAS DEL AYUNTAMIENTO DE MADRID

1. Objeto.

La Política de Identificación y Firma Electrónicas del Ayuntamiento de Madrid determina las condiciones generales aplicables para la identificación y la firma en la relaciones a través de medios electrónicos del Ayuntamiento de Madrid con la ciudadanía, el personal a su servicio y otras Administraciones públicas.

2. Ámbito de aplicación.

1. La política de identificación y firma electrónicas del Ayuntamiento de Madrid se aplica a:

a) Las personas físicas y jurídicas en toda relación a través de medios electrónicos con el Ayuntamiento de Madrid y sus organismos públicos. En particular, en la relación a través de la sede electrónica https://sede.madrid.es.

b) La actividad del Ayuntamiento de Madrid y sus organismos públicos.

c) Los órganos superiores y directivos del Ayuntamiento de Madrid y de sus organismos públicos.

d) Los concejales sin responsabilidades de gobierno del Ayuntamiento de Madrid.

e) Los empleados públicos al servicio del Ayuntamiento de Madrid y de sus organismos públicos.

f) Los vocales vecinos de las juntas municipales de distrito.

2. La política de identificación y firma electróncias del Ayuntamiento de Madrid será interoperable con la política marco de firma electrónica y certificados de la Administración General del Estado y con sus correspondientes ficheros de implementación, según las condiciones establecidas en las normas técnicas de interoperabilidad que resulten de aplicación.

3. Definiciones.

A los efectos de la presente Política se considerará:

3.1 Ciudadanía.

Los sujetos previstos en el apartado 2.1 a).

3.2. Personal al servicio del Ayuntamiento de Madrid.

Los sujetos previstos en el aparado 2.1 c), d), e) y f).

3.3. Trámite.

Cualquier actuación realizada por los sujetos previstos en el apartado 2, mediante la que se pretenda acceder a una información en poder de la Administración municipal, facilitar información a la Administración municipal o realizar cualquier tipo de actuación en el seno de un procedimiento administrativo.

3.4. Sistemas de identificación.

Medios que permiten a la Administración municipal verificar la identidad de quienes efectúan los correspondientes trámites, 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.

3.5. Sistemas de firma.

Medios que permiten a la Administración municipal acreditar la autenticidad de la expresión de la voluntad y consentimiento del firmante, así como la integridad e inalterabilidad del documento que se firma.

3.6. Firma biométrica.

Conjunto de datos biométricos asociados al grafo del firmante, capturados durante el proceso de firma manuscrita sobre dispositivos electrónicos, que pueden asegurar el vínculo entre el documento y la identidad del firmante.

3.7. Firma electrónica.

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. La firma electrónica podrá ser:

a) Avanzada: 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.

b) Cualificada: firma electrónica avanzada creada mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado electrónico cualificado de firma electrónica.

c) No criptográfica: firma electrónica no basada en certificados electrónicos que asocia de forma unívoca un documento con la identidad de una persona, junto

con determinadas evidencias que acreditan el consentimiento y voluntad de firma en un determinado momento.

3.8. Certificado electrónico.

Declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

El certificado electrónico cualificado es un certificado de firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y es expedido por un prestador de servicios incluido en la "Lista de Confianza de prestadores de servicios de certificación".

3.9 Código seguro de verificación (en adelante, CSV).

Código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

3.10. Firma con código seguro de verificación (en adelante, firma con CSV).

Sistema de firma electrónica no criptográfica vinculado a la Administración municipal, órgano o entidad y, en su caso, a la persona firmante del documento, que permite comprobar la integridad del documento firmado mediante el acceso a la sede electrónica del Ayuntamiento de Madrid a través del correspondiente CSV.

4. Normativa aplicable.

La normativa aplicable a la política de identificación y firma electrónicas del Ayuntamiento de Madrid es la siguiente:

a) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

b) Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del

Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

c) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

d) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

e) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

f) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

g) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

h) Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad.

i) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

j) Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.

k) Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.

l) Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

m) Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.

n) Resolución de 19 de julio de 2011, de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.

ñ) Ordenanza de Atención a la Ciudadanía y Administración Electrónica del Ayuntamiento de Madrid, de 26 de febrero de 2019 (en adelante, OACAE).

o) Capítulo VI del Reglamento de Ordenación del Personal del Ayuntamiento de Madrid, de 22 de diciembre de 2005.

5. Estándares internacionales y especificaciones técnicas.

Los estándares internacionales y especificaciones técnicas aplicables a la política de identificación y firma electrónicas del Ayuntamiento de Madrid son los siguientes:

a) ETSI TS 101 733, v.1.6.3, v1.7.3, v.1.8.3 y v.2.2.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).

b) ETSI TS 101 903, v.1.2.2, v.1.3.2, 1.4.2 y v2.1.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

c) ETSI TS 102 778-1 V1.1.1 (2009-07). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES overview – a framework document for PAdES.

d) ETSI TS 102 778-2 V1.2.1 (2009-07). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

e) ETSI TS 102 778-3 V1.1.2 (2009-12). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

f) ETSI TS 102 778-4 V1.1.2 (2009-12). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term – PadES-LTV Profile.

g) ETSI TS 103 172 V2.2.2 (2013-04). Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.

h) ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

i) ETSI TS 101 861 V1.4.1. Time stamping profile.

j) ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

k) ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

l) ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

m) ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

n) IETF RFC 2560, X.509. Internet Public Key Infrastructure Online Certificate Status Protocol– OCSP.

ñ) IETF RFC 3125. Electronic Signature Policies.

o) IETF RFC 3161 actualizada por RFC 5816, Internet X.509. Public Key Infrastructure Time-Stamp Protocol (TSP).

p) IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

q) IETF RFC 5652, RFC 4853 y RFC 3852. Cryptographic Message Syntax (CMS).

r) ITU-T Recommendation X.680 (1997). Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

6. Niveles de seguridad.

6.1. Todo trámite se clasificará en cuatro diferentes niveles de seguridad que determinarán el sistema de identificación y firma electrónicas a utilizar.

6.2. Conforme a los criterios previstos en 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, los niveles de seguridad se clasifican en:

a) Nivel 1. Anónimo.

b) Nivel 2. Bajo.

c) Nivel 3. Medio.

d) Nivel 4. Alto.

7. Criterios generales de identificación y firma electrónicas de la ciudadanía.

7.1. La identificación y firma electrónicas de la ciudadanía se regirá por los siguientes criterios:

a) Con carácter general, para realizar cualquier trámite sólo será necesaria la identificación electrónica. La firma electrónica solo será exigible en aquellos supuestos en los que una norma o acto administrativo expresamente la requieran.

b) Se exigirá el sistema de identificación y, en su caso, de firma electrónica correspondientes al nivel mínimo de seguridad requerido en función del tipo trámite

de que se trate. No obstante, podrán utilizarse voluntariamente sistemas de identificación y, en su caso, de firma electrónica correspondientes a un nivel de seguridad superior al nivel requerido.

c) El nivel de seguridad y el sistema de identificación y, en su caso, de firma electrónica requeridos podrá elevarse durante la realización del trámite en todos aquellos casos que no se realicen en acto único.

Cuando el trámite requiera un desarrollo en varias etapas, podrá ser iniciado con un sistema de identificación y, en su caso, de firma electrónica correspondientes a un nivel mínimo de seguridad y ser exigidos posteriormente sistemas correspondientes a un nivel mayor de seguridad en el momento procedimental oportuno.

d) Deberá conocerse de forma previa al inicio de cada trámite el sistema de identificación y, en su caso, de firma electrónicas requerido. A estos efectos la sede electrónica del Ayuntamiento https://sede.madrid.es, mostrará de forma clara y simple dicha información.

7.2. Los sujetos no obligados a relacionarse por medios electrónicos con la Administración que no dispongan de medios para actuar electrónicamente, podrán ser asistidos para ello por empleados públicos al servicio del Ayuntamiento de Madrid en los términos previstos en la OACAE.

En tales casos, el empleado público actuará mediante el uso de sistemas de identificación y firma de nivel de seguridad 3 o 4 de los que disponga por su condición de empleado público.

8. Sistemas de acceso basados en usuario y clave sin registro previo para uso de la ciudadanía.

Estos sistemas solo se podrán utilizar para la prestación de servicios que requieran nivel de seguridad 2, en los que no sea necesario garantizar la identidad mediante un sistema de identificación o firma. En estos casos, podrán existir medidas organizativas relacionadas con la prestación del servicio realizada que permitan establecer la identidad.

9. Sistemas de identificación y firma electrónicas utilizables por la ciudadanía.

9.1. Sistemas de firma biométrica.

9.1.1. Servirán para la identificación o firma en los trámites que requieran nivel de seguridad 2 o 3.

9.1.2. Los sistemas de firma biométrica asegurarán que en el momento de la firma se captura la información biométrica asociada de manera única al firmante y que dicha información es incorporada al documento electrónico, garantizando su integridad

mediante el sellado electrónico con un sello emitido a nombre del Ayuntamiento de Madrid o un órgano superior o directivo del mismo.

9.2. Sistemas de identificación y firma electrónicas no criptográficos.

9.2.1. Los sistemas de clave concertada existentes en la plataforma Cl@ve servirán para la identificación y firma en los trámites que requieran nivel de seguridad 2 o 3.

9.2.2. El sistema de firma con CSV, con acreditación de identidad, voluntad y consentimiento, servirá para la identificación y firma en los trámites que requieran nivel de seguridad 2 o 3, siempre y cuando cumpla con los siguientes requisitos:

a) Verificación de la información a firmar y consentimiento expreso.

b) Vinculación de datos mediante fecha y hora de la identificación; nombre y apellidos; NIF/NIE del usuario; mecanismo de identificación usado: fecha y hora de la firma; algoritmo resumen usado, valor para el documento a firmar por el usuario y CSV.

9.2.3. La generación del CSV del Ayuntamiento de Madrid garantizará el cumplimiento de los requisitos funcionales previstos en el artículo 45.7 OACAE y, en particular, los siguientes:

a) Vincular de manera unívoca un documento, el firmante y las evidencias asociadas. Esta relación unívoca es permanente.

b) Ser único.

c) Ser aleatorio, no pudiéndose dar el caso de dos documentos con códigos seguidos. El espacio de códigos generado por el algoritmo será amplio, existiendo discontinuidades entre los códigos generados y evitando códigos secuenciales.

d) Ser consultable en la Sede Electrónica del Ayuntamiento de Madrid.

e) Disponer de un tiempo de generación muy bajo, para no penalizar el rendimiento de los sistemas.

f) Utilizar algoritmos estándares seguros para la generación de códigos no secuenciales y codificación alfanumérica.

9.2.4. Los requisitos previstos en el punto 9.2.3 serán también de aplicación al CSV que se genere para documentos no firmados electrónicamente.

9.3. Sistemas de identificación y firma electrónicas basados en certificados electrónicos.

Servirán para la identificación y firma en los trámites que requieran nivel de seguridad 2.

Si los certificados electrónicos son cualificados servirán para la identificación y firma en los trámites que requieran nivel de seguridad 3 o 4.

10. Sistemas de identificación y firma utilizables por el Ayuntamiento de Madrid y sus organismos públicos.

10.1. Los sistemas de identificación y firma utilizables por el Ayuntamiento de Madrid y sus organismos públicos se rigen por lo previsto en el capítulo II del título VI de la OACAE.

10.2. De conformidad con el artículo 61 OACAE, en la actuación administrativa automatizada, el Ayuntamiento de Madrid y sus organismos públicos utilizarán sellos electrónicos de órgano emitidos por un prestador de servicios de certificación electrónica cualificado o el sistema de firma con CSV previsto en el punto 9.2.2.

11. Sistemas de identificación y firma utilizables por el personal al servicio del Ayuntamiento de Madrid.

11.1. La utilización de los sistemas de identificación y firma por el personal al servicio del Ayuntamiento de Madrid se rige por lo previsto en el capítulo VI del Reglamento de Ordenación del Personal del Ayuntamiento de Madrid, de 22 de diciembre de 2005.

11.2. El personal al servicio del Ayuntamiento de Madrid dispondrá de certificados electrónicos de empleado público emitidos por un prestador de servicios de certificación electrónica cualificado.

11.3. Los certificados electrónicos del personal al servicio del Ayuntamiento de Madrid podrán emitirse con número de idenficación profesional en los casos legalmente establecidos.

11.4. Cuando el personal al servicio del Ayuntamiento de Madrid actúe en el ejercicio de sus funciones, utilizará los certificados electrónicos de empleado público o el sistema de identificación y firma con CSV previsto en el punto 9.2.2.

11.5. En caso de imposibilidad técnica de utilización de los sistemas previstos en el punto 11.4, podrá autorizarse el uso voluntario de certificados electrónicos cualificados estrictamente personales de los que disponga dicho personal.

11.6. Relaciones internas.

11.6.1. En el ámbito de sus relaciones internas con el Ayuntamiento de Madrid, el personal a su servicio se considerará identificado con carácter general mediante el

usuario y contraseña personal del directorio corporativo de usuarios o mediante su cuenta personalizada de correo electrónico.

Cuando resulte necesario, los sistemas y aplicaciones podrán requerir el número de empleado u otra información propia de la relación laboral para mayor contraste de la identificación, sin perjuicio de la posibilidad de utilizar los sistemas de identificación y firma electrónicas previstos en el punto 11.4.

11.6.2. Cuando actúen como interesados en procedimientos de gestión de recursos humanos, los sistemas y aplicaciones, en los trámites que así lo requieran según los niveles de seguridad establecidos, podrán requerir códigos de usuario con contraseña personalizable, que permitan acreditar la identidad, autenticidad de la expresión de la voluntad y el consentimiento del personal usuario, la integridad e inalterabilidad del documento, así como la trazabilidad de las actuaciones realizadas, sin perjuicio de la posibilidad de utilizar los sistemas de identificación y firma electrónicas previstos en el punto 11.4.

11.7. Conservación y uso.

El personal al servicio del Ayuntamiento de Madrid municipal será responsable del uso, custodia y salvaguarda de la confidencialidad y privacidad del uso de los sistemas de identificación y firma electrónicas que le hayan sido facilitados para el ejercicio de sus funciones.

Tales sistemas no podrán ser utilizados para fines personales.

12. Portafirmas.

12.1. El Ayuntamiento de Madrid dispondrá un sistema de portafirmas que permita la firma electrónica basada en certificados electrónicos desde el puesto de trabajo y desde dispositivos móviles.

12.2. Con carácter general, el sistema de portafirmas será la herramienta de firma electrónica que se utilizará por parte del personal al servicio del Ayuntamiento de Madrid para firmar electrónicamente documentos. No obstante, podrán habilitarse otras herramientas de firma electrónica para procedimientos, trámites o documentos concretos.

12.3. Los documentos firmados mediante el portafirmas u otras herramientas de firma electrónica serán accesibles desde la sede electrónica o la intranet municipal a través del CSV correspondiente a cada documento firmado.

13. Gestión de certificados electrónicos.

13.1. La autoridad de certificación emisora de los certificados electrónicos que en cada momento provea al Ayuntamiento de Madrid, será la responsable de definir las políticas de gestión de los certificados emitidos.

13.2. En el marco de las relaciones que se desarrollen con la autoridad de certificación correspondiente, se establecerá una autoridad de registro del Ayuntamiento de Madrid para coordinar los trabajos de emisión de certificados.

La autoridad de registro dependerá del órgano competente en materia de firma electrónica.