ENCARGO QUE REALIZA LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS A LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA, PARA LA PRESTACIÓN DE SERVICIOS, TÉCNICOS Y DE SEGURIDAD, APLICABLES A LA CERTIFICACIÓN Y FIRMA ELECTRÓNICA Y EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

En Madrid,

REUNIDOS

De una parte, **Dña. Mar España Martí,** en nombre y representación de **Agencia Española de Protección de Datos –en adelante AEPD-**, (entidad con NIF Q2813014D y domicilio social en c/ Jorge Juan n.º 6 28001-Madrid), en su calidad de Directora de la misma, nombrada por Real Decreto 715/2015 de 24 de julio (BOE de 25-7-2015) y haciendo uso de las facultades que tiene conferidas por los artículos 12 y 13 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Y de otra, doña Lidia Sánchez Milán, Directora General de la Fábrica Nacional de Moneda y Timbre–Real Casa de la Moneda, nombrado por Real Decreto 270/2020, de 4 de febrero (BOE núm. 31, de 5 de febrero), en representación de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda [artículo 19.2 del Real Decreto 114/1999, de 25 de junio, por el que sea aprueba el Estatuto de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (BOE núm. 161, de 7 de julio)] con domicilio en Madrid, calle Jorge Juan, 106 (Código de identificación Fiscal Q28/26004J).

La Entidad está regulada por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por su Estatuto, aprobado por el Real Decreto 1114/1999, de 25 de junio; estando adscrita a la Subsecretaría de Hacienda y Función Pública, en virtud del artículo 12.12.b) del Real Decreto 1113/2018, de 7 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda.

Ambas partes, reconociéndose la capacidad legal y competencia necesarias para formalizar el presente Encargo,

EXPONEN

PRIMERO. La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece las bases de regulación de la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, tanto para el sector público como el privado. El artículo 4 de esta Ley establece el empleo de la firma electrónica en el ámbito de las Administraciones Públicas para que, con el objetivo básico de salvaguardar las garantías de cada procedimiento, se puedan establecer condiciones adicionales, como la imposición de fechas electrónicas sobre los documentos de la misma naturaleza, que integren un expediente administrativo.

En este ámbito, ha de tenerse en cuenta la efectiva aplicación, desde el 1 de julio de 2016, del "REGLAMENTO (UE) nº 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 la que se deroga la Directiva 1999/93/CE", que es de directa aplicación en los Estados miembros. Se encuentra en tramitación la modificación de la Ley española para adaptarse a este Reglamento.

La Disposición adicional cuarta de la Ley 59/2003 constata la especialidad en la regulación que afecta a la actividad de la FNMT-RCM, al expresar que, lo dispuesto en esa Ley, se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

SEGUNDO. El citado artículo 81 de la Ley 66/1997, de 30 de diciembre, faculta a la FNMT-RCM para prestar los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia en la emisión y recepción de comunicaciones y documentos a través de técnicas electrónicas, informáticas y telemáticas (EIT), entre otros, entre las personas físicas y jurídicas con la Administración General del Estado y con los organismos públicos vinculados o dependientes de ella y de estos sujetos públicos entre sí.

Tal artículo, modificado y ampliado mediante las Leyes 55/1999, 14/2000, 44/2002, 53/2002 y 59/2003, trae causa del mandato para el impulso del empleo y la aplicación de técnicas y medios EIT, en el desarrollo de la actividad y el ejercicio de las competencias de las Administraciones Públicas, según estableció el artículo 45.1 de la derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y que ahora se regula en los artículos 17, 26 y 27 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Este mismo artículo 81, en su apartado cinco, señala que, con la finalidad de extender los servicios dados por la FNMT-RCM, que sería el ámbito de este instrumento, la Entidad podrá celebrar convenios con las diferentes Administraciones públicas, entidades y organismos públicos vinculados o dependientes, constituyendo, el referido artículo 81 y legislación de desarrollo antes citada, norma especial.

En relación con las actividades de identificación y registro, la FNMT-RCM podrá celebrar convenios con personas, entidades y corporaciones que ejerzan funciones públicas, en los que se establezcan las condiciones en las que éstas puedan participar en tales actividades.

TERCERO. El Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81, antes citado, regula el régimen de prestación de servicios de seguridad por la FNMT-RCM en la emisión y recepción de comunicaciones y escritos a través de medios y técnicas electrónicas, informáticas y telemáticas. Su artículo 6, faculta a la FNMT-RCM para convenir con las entidades incluidas en su ámbito de aplicación, entre las que se encuentra la AEPD, los términos que deben regir la prestación de sus

servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos.

CUARTO. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas reconoce a los ciudadanos su derecho a relacionarse, preferentemente y de forma electrónica, con las Administraciones Públicas, con el fin de contribuir a la extensión y consolidación de la Administración Electrónica. Para ello, la FNMT-RCM en colaboración con las diferentes Administraciones, presta servicios técnicos y administrativos necesarios para la identificación y autenticación de los intervinientes en las comunicaciones electrónicas con y entre las Administraciones Públicas, a través del uso de certificados de firma electrónica para funcionarios y demás empleados públicos, certificados de sede electrónica y certificados de sello electrónico para la actuación administrativa automatizada, en los que las Administraciones y organismos actúan, en sus registros y sedes electrónicas, a través de las oficinas de registro propias encargadas de acreditar y constatar los requisitos y condiciones especiales de utilización de estos servicios de certificación electrónica a prestar por la FNMT-RCM.

La Ley 39/2015, de 1 de octubre, y el Real Decreto 1671/2009 de 6 de noviembre (que desarrollaba la derogada Ley 11/2007 de 22 de Junio de acceso electrónico de los ciudadanos y que mantiene parcialmente su vigencia en virtud de la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, y la Disposición derogatoria única de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público) facilitan a los ciudadanos la efectiva realización de los derechos reconocidos en la Ley, a través del triple objetivo del Real Decreto:

- evitar que la nueva regulación imponga una renovación que impida la pervivencia de técnicas de gran arraigo;
- facilitar la implantación y adaptación de las organizaciones a las nuevas funciones y procedimientos, e
- impedir que la opción rígida de determinadas soluciones dificulte la incorporación futura de nuevos servicios y aplicaciones.

Este Real Decreto, en los Capítulos I y II de su Título VI, regula la materia relativa a los documentos electrónicos y sus copias, en especial, documentos administrativos electrónicos, archivo electrónico de documentos, expediente electrónico y digitalización.

Por su parte, la Ley 40/2015, de 1 de octubre, recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrollaba parcialmente la anterior. La Ley establece que la utilización de los medios electrónicos ha de ser lo habitual, como la firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada. Se establece, asimismo, la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos, previsión que se desarrolla posteriormente en el título referente a la cooperación interadministrativa mediante una regulación específica de las relaciones electrónicas

entre las Administraciones. Para ello, también se contempla como nuevo principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos.

El Capítulo V del Título Preliminar de la Ley 40/2015, de 1 de octubre, regula, específicamente, el funcionamiento electrónico del sector público, integrado por la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local y el Sector Público Institucional.

QUINTO. De acuerdo con lo establecido en los artículos 6 y 32 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, y con las acotaciones y aclaraciones de la numerosa jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, están excluidos de la aplicación de la Ley de Contratos del Sector Público los negocios jurídicos en cuya virtud se encargue una determinada prestación a una entidad que tenga atribuida la condición de medio propio y servicio técnico del poder adjudicador correspondiente, como la FNMT-RCM que, según su Estatuto, es medio propio de la Administración General del Estado, así como de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada, vinculados o dependientes de aquélla, pues realiza la parte esencial de su actividad con esta administración que mantiene un control análogo al que ejerce sobre sus propios servicios, por lo que a la FNMT-RCM se le pueden conferir de encargos de conformidad con los artículos antes citados.

SEXTO. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda es una entidad pública empresarial dependiente de la Administración General del Estado y se encuentra adscrita al Ministerio de Hacienda, a través de la Subsecretaría de este departamento, que ejerce la dirección estratégica y el control de eficacia de la Entidad. Esta dependencia se recoge en el artículo 12.12.b) del Real Decreto 1113/2018, de 7 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda.

El artículo 2 del Estatuto de la FNMT-RCM, aprobado mediante el Real Decreto 1114/1999, de 25 de junio, reconoce y establece, como uno de sus fines (fijados por el artículo 81, citado en el expositivo segundo), la prestación —en el ámbito de las Administraciones Públicas, o sus Organismos Públicos, vinculados o dependientes— de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) así como la expedición, fabricación y suministro de títulos o certificados de usuario (y sus soportes), de acuerdo con lo que determinen las disposiciones legales correspondientes.

Por su parte, el apartado 7 del artículo 2 y el apartado 2 del artículo 3 de su Estatuto, según redacción dada por el artículo único del Real Decreto 336/2014, de 25 de junio, configura a la FNMT-RCM como medio propio y servicio técnico de la Administración General del Estado, así como de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada, en los términos de la Ley 9/2017, de 8 de noviembre, (LCSP) y de su Estatuto.

SÉPTIMO. La AEPD, en el marco de desarrollo de sus competencias, presta determinados servicios soportados por técnicas y medios electrónicos, informáticos y telemáticos aplicados a determinados procedimientos administrativos. Estos servicios deben contar con las debidas garantías de seguridad conformes con las disposiciones legales y en orden a garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios EIT. Por otra parte, también se requiere la identificación electrónica de la AEPD y autenticación del ejercicio de su competencia, de conformidad con la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

OCTAVO. Que, en virtud de las razones ahora expuestas, se ha considerado que las relaciones administrativas, prestacionales y de colaboración entre la AEPD y la FNMT-RCM, se instrumenten a través de un encargo, al margen de una relación estrictamente contractual, en la que la propia Administración realiza sus funciones con sus propios medios, o los de entidades sobre las que la Administración, que efectúa el encargo, ostenta un control análogo al que ejerce sobre sus propios servicios (en este caso, medios propios personificados), de acuerdo con lo dispuesto en el art. 32 de la LCSP. Estas actividades públicas y de interés general podrían también instrumentarse a través de las encomiendas de gestión reguladas en el artículo 11 de la Ley 40/2015, de 1 de octubre.

Con objeto de racionalizar el gasto de la prestación de las actividades que la FNMT-RCM viene realizando en el ámbito de Administración Electrónica para la Administración General del Estado, así como en el de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada, vinculados o dependientes de la misma, está vigente una encomienda general suscrita entre el Ministerio de Hacienda y la FNMT-RCM, para unificar las diferentes encomiendas que la Entidad tiene formalizadas en ese ámbito y dar servicio completo a toda la AGE y su Sector Público Institucional (según su ámbito de aplicación).

(...)

Estando ambas partes interesadas en procurar la máxima extensión de la Administración Electrónica para facilitar a los ciudadanos y Administraciones las relaciones a través de las técnicas y medios electrónicos, informáticos y telemáticos (EIT), y de conformidad con lo previsto en este expositivo, se procede a la formalización del presente Encargo con arreglo a las siguientes

CONDICIONES

PRIMERA. OBJETO

1.1.- Constituye el objeto del presente encargo la realización, por parte de la FNMT-RCM a la AEPD, de las siguientes actividades:

a) Servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos

producidos a través de técnicas y medios EIT en el ámbito de actuación de la AEPD, en las condiciones técnico-administrativas que, en las siguientes condiciones se estipulan, y se detallan en el Capítulo I, del Anexo I, de este Encargo.

b) Servicios relativos a la identificación electrónica de las Administraciones Públicas y autenticación del ejercicio de su competencia, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y, en concreto, las actividades que se enumeran en la siguiente condición y en el Capítulo III, del Anexo I, de este Encargo.

1.2.- La FNMT-RCM también prestará a petición de la AEPD cualquiera, o la totalidad, de los servicios adicionales complementarios y/o suministros que, al efecto, se enumeran en los apartados a) y b) de la siguiente condición y en el Capítulo II, del mismo Anexo I, de este Encargo.

SEGUNDA. PRESTACIONES Y ÁMBITO DE APLICACIÓN

2.1.- Para servicios del ámbito del artículo 81.

La FNMT-RCM prestará servicios EIT a las personas que tengan la condición de usuarios de acuerdo con la normativa vigente y las condiciones de este Encargo, cuando los usuarios se relacionen con la AEPD en el marco de sus respectivas competencias, con sujeción a lo establecido en las normas de aplicación y en la Declaración de Prácticas de Certificación (y su Política y Prácticas Particulares), accesibles en la dirección electrónica: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion, los servicios de identificación electrónica y autenticación de documentos electrónicos para los usuarios que se indican a continuación.

Concretamente, las actividades a desplegar son:

- Expedición y gestión del ciclo de vida de certificados de usuario para personas físicas, a través de la AC USUARIOS.
La FNMT-RCM proporcionará instrumentos de identificación, acreditación y firma para asegurar las comunicaciones en el ámbito EIT, como son los certificados de firma electrónica, a las personas físicas que actúan como interesados en el procedimiento administrativo de acuerdo con la normativa vigente y las condiciones del presente encargo, con las administraciones destinatarias de los servicios previstos en el presente encargo. A tal efecto, los Departamentos, organismos y entidades del sector público destinatarios de los servicios admiten los certificados electrónicos expedidos en virtud de del presente encargo por la FNMT-RCM, en calidad de Prestador Cualificado de Servicios de Confianza, como sistemas de identificación electrónica que permiten acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados en el procedimiento administrativo, así como la creación de firmas electrónicas.

- Gestión del ciclo de vida de certificados de representante para personas jurídicas, para administradores únicos y solidarios y para entidades sin personalidad jurídica, a través de la AC REPRESENTACIÓN.

Así mismo, la FNMT–RCM dará acceso a la funcionalidad de los certificados electrónicos de representante de persona jurídica y entidad sin personalidad jurídica, a solicitud de la Administración General del Estados o de los organismos y entidades del sector público vinculadas o dependientes de la misma incluidos en este encargo, como medio de identificación y firma electrónica en su relación con el resto de Administraciones Públicas que los admitan para tales fines y otros supuestos admitidos por el ordenamiento.

A tal efecto, la AEPD asume que los certificados (títulos de usuario) que expida la FNMT-RCM son universales y que, por tanto, servirán para las relaciones jurídicas que mantengan los usuarios con las diferentes Administraciones públicas y, en su caso, en el ámbito privado que admitan la utilización de estos certificados, en sus registros, procedimientos y trámites. De igual forma, los certificados que haya expedido o expida la FNMT-RCM, para otros órganos, organismos y administraciones en el ámbito público de actuación, podrán ser utilizados por los usuarios en sus relaciones con la AEPD.

2.2.- Para servicios del ámbito de la Ley 40/2015.

La FNMT-RCM, a los efectos de lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, prestará en los términos de la citada Ley y en los señalados en el Capítulo III, del Anexo I de este Encargo, y con sujeción a lo establecido en la normas de aplicación y en la Declaración de Prácticas de Certificación (y su Política y Prácticas Particulares), accesibles en la dirección electrónica: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion, los siguientes servicios de identificación electrónica y autenticación de documentos electrónicos de las Administraciones Públicas:

- número ilimitado certificados de Empleado Público.
- 1 certificado de sede electrónica.
- 3 certificados de sello electrónico de administración pública.
- número ilimitado certificados de Empleado Público en la nube (Firma Centralizada).

- Emisión de Sellos de Tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo del presente encargo, previa petición de la AEPD a través de la Infraestructura Pública de Sellado de Tiempo de la FNMT-RCM, sincronizada mediante convenio con el Real Instituto y Observatorio de la Armada (ROA), como órgano competente del mantenimiento del Patrón Hora en España.

2.3.- Servicios complementarios.

Estos servicios podrán prestarse tanto en el ámbito del artículo 81 de la Ley 66/1997, como en el de la Ley 40/2015 y se caracterizan por ser complementarios de los servicios señalados anteriormente:

- 5 certificados de componente

2.4.- Las condiciones económicas de las actividades a desarrollar en relación con servicios, actividades o suministros especificados en esta condición, se detallan en el Anexo II de tarifas.

~~2.5. ...~~

TERCERA. OBLIGACIONES DE LAS PARTES PARA LA PRESTACIÓN EFECTIVA DE LOS SERVICIOS OBJETO DEL ENCARGO

1.- Para la prestación efectiva de los servicios objeto del Encargo, la FNMT-RCM se compromete a:

- Aportar la infraestructura técnica, organizativa y de seguridad relacionada en los Anexos I y II de este Encargo.

- Aportar los derechos de propiedad industrial e intelectual necesarios, garantizando su uso pacífico. La FNMT-RCM, excluye cualesquiera licencias o sublicencias, a terceras partes o a la AEPD para aplicaciones y sistemas de la AEPD, o de terceros, distintas de las aportadas directamente por la FNMT-RCM.

- Prestar la asistencia técnica que se precise con objeto de facilitar a la AEPD la información necesaria para el buen funcionamiento de los sistemas, de conformidad con lo establecido en los Anexos de este Encargo.

- Actualizar tecnológicamente los sistemas, de acuerdo con el estado de la técnica y las disponibilidades presupuestarias de la FNMT-RCM, sin perjuicio de la aprobación de los requisitos técnicos correspondientes por la Comisión de Estrategia TIC o, en su caso, por el órgano competente.

- Previa petición de la AEPD, la FNMT-RCM, también realizará la Emisión de Sellos de Tiempo en las comunicaciones electrónicas, informáticas y telemáticas que tengan lugar al amparo del presente Encargo, a través de la Infraestructura Pública de Sellado de Tiempo de la FNMT-RCM, sincronizada mediante convenio con el Real Instituto y Observatorio de la Armada (ROA), como órgano competente del mantenimiento del Patrón Hora en España.

- Aportar la tecnología necesaria para que las obligaciones de la AEPD, puedan ser realizadas; en particular, las aplicaciones necesarias para la constitución de las Oficinas de Registro y acreditación y la tramitación de las solicitudes relativas a los certificados electrónicos. Tales aplicaciones serán compatibles en función de los avances tecnológicos y el estado de la técnica.

- Tener disponible para consulta de la AEPD y de los usuarios una Declaración de Prácticas de Certificación (DPC), que contendrá, al menos, las especificaciones establecidas en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Tal DPC, estará disponible en la dirección electrónica (URL) expresada en la condición Segunda. Esta DPC, podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, por razones legales o de procedimiento, estando siempre disponible la vigente y el histórico de versiones en las direcciones electrónicas especificadas en esta

condición. Hay que tener en cuenta la parte general de la DPC y, para cada tipo de certificado o ámbito de actuación, las Políticas y Prácticas de Certificación Particulares aplicables específicamente, así como las Declaraciones Informativas PDSs, los Términos y Condiciones y los Perfiles de Certificados.

- Emisión de informes, a petición de la AEPD y de los Juzgados, Tribunales y, en su caso, órganos administrativos y/o supervisores competentes, acreditativos de la actividad de certificación realizada por la FNMT-RCM en aplicación de este Encargo.

Los medios técnicos y tecnología empleados por la FNMT-RCM permitirán demostrar la fiabilidad del servicio de certificación electrónica, la constatación de la fecha y hora de expedición, suspensión o revocación de un certificado, la fiabilidad de los sistemas y productos (que contarán con la debida protección contra alteraciones, así como con los niveles de seguridad técnica y criptográfica idóneos dependiendo de los procedimientos donde se utilicen), la comprobación de la identidad del titular del certificado, a través de las Oficinas de Registro y acreditación autorizadas y, en su caso, —exclusivamente frente a la parte o entidad a través de la cual se ha identificado y registrado al titular del certificado— los atributos pertinentes, así como, en general, las actuaciones que resulten de aplicación de conformidad con la normativa comunitaria o nacional correspondiente.

No obstante lo anterior, en la prestación de servicios del ámbito de la Ley 40/2015, las Oficinas de Registro, por las especialidades del derecho administrativo y de gestión y de conformidad con el artículo 11 del Real Decreto 1317/2001, de 30 de noviembre, no dependerán directamente de la FNMT-RCM sino del órgano, organismo o entidad de la que orgánicamente dependan, sin perjuicio de las funciones de comprobación, coordinación, control de gestión y de los protocolos y directrices sobre registro y acreditación que realice la FNMT-RCM, en su condición de Prestador de Servicios de Certificación.

La FNMT-RCM se compromete, en el desarrollo y ejecución del Encargo a la aplicación, cuando sea procedente de acuerdo con el tipo de actividad realizada, de las disposiciones y recomendaciones relativas a los ámbitos normativos o programáticos sobre protección del medio ambiente, prevención de riesgos laborales, igualdad y no discriminación.

2.- Por su parte, la AEPD se compromete a:

- Emitir el recibo de presentación, firmado electrónicamente, donde se haga constancia expresa de la fecha y hora de recepción de las comunicaciones recibidas, de conformidad con lo dispuesto en la normativa aplicable.

- Conservar las notificaciones, comunicaciones o documentación emitida y recibida en las transacciones durante el tiempo pertinente para hacer valer los derechos de las partes.

- Cifrar las comunicaciones emitidas y recibidas.

- Realizar las actividades de identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia de los atributos correspondientes, de los titulares de los certificados, así como del cargo y competencia de los firmantes/custodios correspondientes. Todo ello, a través de la Oficina de Registro y acreditación designada ante la FNMT-RCM, utilizando los procedimientos establecidos por esta Entidad, que figuran en la aplicación de Registro (aplicación Web) y en la DPC de la FNMT-RCM. Tales procedimientos, son documentos sujetos a verificaciones y auditorías por lo que podrán ser modificados por la FNMT-RCM a los efectos de mejorar el servicio.

- Conservar, a su vez, durante, al menos, quince años o el tiempo máximo que establezca la Ley de Firma Electrónica vigente en cada momento, los formularios y documentos donde constan las condiciones para la solicitud, revocación y suspensión, en su caso, de certificados electrónicos emitidos por la FNMT-RCM, así como su remisión electrónica a la FNMT-RCM, de conformidad con lo establecido en los procedimientos de registro que constan en la dirección electrónica: https://www.sede.fnmt.gob.es/registro-inicio o la que la sustituya.

La AEPD se compromete, en el desarrollo y ejecución del presente Encargo, a la aplicación, cuando sea procedente de acuerdo con el tipo de actividad realizada, de las disposiciones y recomendaciones relativas a los ámbitos normativos o programáticos sobre protección del medio ambiente, prevención de riesgos laborales, igualdad y no discriminación.

3.- Oficinas de Registro.

El número y ubicación de las Oficinas de Registro y Acreditación donde se llevarán a cabo las actividades de identificación, recepción y tramitación de solicitudes de expedición de certificados electrónicos será informado por la AEPD a la FNMT-RCM, así como cualquier modificación o alteración de dicha relación o de la ubicación de las Oficinas.

Las aplicaciones informáticas necesarias para llevar a cabo las actividades de acreditación e identificación serán facilitadas por la FNMT-RCM a la AEPD a través de los permisos correspondientes. Tales aplicaciones serán tecnológicamente compatibles en función de los avances tecnológicos y el estado de la técnica.
Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos aprobados por la FNMT – RCM y a los procedimientos recogidos en la Declaración de Prácticas de Certificación de la Entidad, antes referenciadas, así como a los procedimientos de registro de la FNMT-RCM.

* Para los servicios del artículo 81 de la Ley 66/1997.

La AEPD podrá disponer de una red de Oficinas de Registro y acreditación que contarán con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados exigirá la comprobación de su identidad y de su voluntad de que sea

expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, y se verificará de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable y de conformidad con la DPC General y la específica Política y Prácticas de Certificación particulares correspondientes a estos certificados (AC Usuarios y, en su caso, AC Representación), disponibles para consulta en la dirección electrónica recogida en la condición Segunda.

Estas Oficinas de Registro y acreditación de la AEPD, se integrarán en la Red de Oficinas de Registro y acreditación a las que los ciudadanos pueden dirigirse para obtener un certificado electrónico expedido por la FNMT-RCM con observancia de lo dispuesto en la normativa aplicable. Las acreditaciones realizadas por las personas, entidades y corporaciones a que se refiere el apartado nueve del artículo 81 de la Ley 66/1997, de 30 de diciembre, citada, y por los diferentes órganos y organismos públicos de la Red de Oficinas de Registro y acreditación, surtirán plenos efectos y serán válidas para su aceptación por cualquier administración pública que admita los certificados de emitidos por la FNMT-RCM.

* Para los servicios de la Ley 40/2015.

Las Oficinas de Registro de la AEPD, para el ámbito de la Ley 40/2015, son de orden interno de cada administración u organismo correspondiente y determinarán la identidad y competencia de las Administraciones y la de los diferentes firmantes/custodios designados por las Administraciones, entidades y organismos vinculados o dependientes suscriptores de los certificados, de conformidad con la DPC General y la específica Política y Prácticas de Certificación particulares de Administración Pública, disponibles para consulta en las direcciones electrónicas de la condición Segunda.

A tal efecto, la AEPD dispondrá de las Oficinas de Registro y acreditación que considere necesarias y adecuadas para la acreditación de este tipo de certificados y deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM y realizar las solicitudes de emisión de los certificados. En las Oficinas de Registro, para acreditar e identificar a los titulares y custodios de los certificados, se exigirá la comprobación de su identidad, del cargo y de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente y de la voluntad del titular del certificado, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

En caso de que los jueces y tribunales u otros órganos y organismos con competencia a estos efectos, soliciten a la FNMT-RCM la aportación de cualquier dato identificativo sobre cualesquiera certificados emitidos con arreglo a la Ley 40/2015, de 1 de octubre, la Oficina de Registro deberá colaborar con la FNMT-RCM aportando la información solicitada antes del plazo que figure en la petición. Todo ello, sin perjuicio de la aplicación de las normas sobre secretos oficiales, seguridad y defensa, cuestión que se evaluará caso a caso.

CUARTA. PLAZO DE DURACIÓN

El presente encargo entrará en vigor el 1 de octubre de 2019 y su vigencia se extenderá un año, hasta el 30 de septiembre de 2020. La duración del encargo se prorrogará por periodos anuales sucesivos salvo que la AEPD decida resolver o finalizar este encargo mediante notificación expresa a la FNMT-RCM con antelación al plazo de vencimiento inicial del mismo, o de cualquiera de sus prórrogas, siendo estas prórrogas asumidas por la FNMT-RCM.

La contratación de las actividades previstas en este encargo, más allá de su duración inicial y, en su caso, su prórroga o sus prórrogas, solamente podrá realizarse por nuevo Encargo.

QUINTA. RÉGIMEN DE LAS PRESTACIONES

Ámbito objetivo

La prestación de los servicios EIT a que se refiere la condición primera, se realizará atendiendo a lo establecido en los Capítulos I y II del Anexo I, para los servicios relativos al artículo 81 de la Ley 66/1997, y atendiendo a lo establecido en el Capítulo III, del Anexo I, para los servicios relativos al ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A tal efecto, ambas partes se comprometen a asumir las obligaciones necesarias a este fin. Igualmente, la AEPD se obliga a velar frente a los usuarios por el cumplimiento de las obligaciones que le correspondan como encargada de la identificación, acreditación y registro de usuarios y de los funcionarios y empleados públicos, firmantes/custodios, así como de la recepción y tramitación de solicitudes de expedición, revocación y, en su caso, suspensión de cualesquiera certificados electrónicos previstos en este Encargo y sus Anexos.

Medidas de Seguridad

La FNMT-RCM se compromete a adoptar cuantas medidas sean necesarias en orden a mantener el secreto de las características técnicas de seguridad que deben reunir los productos, servicios y procedimientos aplicados, tanto en sus instalaciones y personal, como, en su caso, en las de entidades colaboradoras, aplicando, de conformidad con la normativa especial correspondiente, los Esquemas Nacionales de Seguridad e Interoperabilidad y las Instrucciones Internas de Contratación de la Entidad, así como las obligaciones de confidencialidad pertinentes, restringiendo la información y la publicidad de los diferentes elementos de seguridad, según los estándares aplicables y, en general, realizando la actividad encargada implantando medidas especiales de seguridad, de conformidad con el estado de la técnica.

SEXTA. TARIFAS Y CONDICIONES DE PAGO

1.- TARIFAS EN MATERIA DE CERTIFICACIÓN ELECTRÓNICA SOBRE LA BASE DEL ART. 81 (CIUDADANOS / EMPRESAS).

En caso de ser solicitada de forma expresa, la FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en la AEPD (según el Capítulo I, del Anexo I, y calculada de acuerdo con el artículo 30 del Estatuto de la FNMT-RCM), la cantidad por cada de vigencia del encargo será de mil euros (1.000,00€ / año), impuestos no incluidos.

Tanto durante el primer año, como en el de las eventuales prórrogas, si hubiera petición expresa, por parte de la AEPD, de extensión de otras actividades o funcionalidades de entre las recogidas en el Capítulo II, del Anexo I, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas de los Capítulos I y II, del Anexo II, de Precios del presente Encargo.

2.- TARIFAS EN MATERIA DE INTERMEDIACIÓN ADMINISTRATIVA SOBRE LA BASE DE LA LEY 40/2015 (EMPLEADO/SEDE/SELLO).

La FNMT-RCM, como compensación por las actividades desarrolladas, percibirá por su actividad de extensión de la Administración Electrónica en la AEPD dentro del ámbito de la Ley 40/2015 recogida en el Capítulo III del Anexo I, la cantidad por cada de vigencia del encargo será de seis mil quinientos euros (6.500,00€ / año), impuestos no incluidos.

Tanto durante el primer año, como en el de las eventuales prórrogas, si hubiera petición expresa, por parte de la AEPD, de extensión de otras actividades o funcionalidades de entre las recogidas en el Capítulo III, del Anexo I, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas del Capítulo III del Anexo II, de Precios del presente Encargo.

3.- REEMBOLSO TOTAL.

La cantidad total de compensación a la FNMT-RCM por aplicación del Encargo en por cada de vigencia del encargo asciende a siete mil quinientos euros (7.500,00€ / año), impuestos no incluidos. La retribución de los servicios encargados para las prórrogas anuales sucesivas no experimentará variación con respecto de los importes de la anualidad inicial.

Esta cantidad se obtiene de la suma de las cantidades establecidas en los apartados 1 y 2 anteriores, sin perjuicio de su incremento por petición de funcionalidades adicionales. Para sucesivos años, se aplicará el mismo criterio en función de las compensaciones a percibir, servicios solicitados y prórrogas del Encargo.

La contraprestación a percibir por la FNMT-RCM en las siguientes anualidades serán:

- Para el ejercicio 2019, de 0,00 euros, IVA no incluido.
- Para el ejercicio 2020, de 7.500,00 euros, IVA no incluido; 9.075,00 euros IVA incluido.

Existe presupuesto y/o certificación de crédito nº 13301220310000123 con fecha 12 de febrero de 2020 por 9.075,00 euros para el ejercicio 2020.

4.- CONSIDERACIÓN DE LAS CONTRAPRESTACIONES

Las contraprestaciones establecidas en este Encargo y sus Anexos, tienen la consideración de tarifas a los efectos previstos en el artículo 32 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, una vez sea autorizada la formalización del presente Encargo por el órgano directivo de adscripción de la FNMT-RCM, la Subsecretaría de Hacienda, de conformidad con lo dispuesto en el artículo 3.2 del Estatuto de esta Entidad. No obstante, la FNMT-RCM quedará obligada a aceptar cualesquiera otras tarifas que sean impuestas por esta Subsecretaría, en cuanto órgano directivo de adscripción de la Entidad, en relación con el número de administraciones destinatarias, de las disponibilidades presupuestarias y del volumen de los servicios prestados. Todo ello teniendo en cuenta la equiparación entre el coste del producto o servicio y el precio a repercutir, el cual comprenderá necesariamente un porcentaje de actualización tecnológica de la FNMT-RCM, que podrá oscilar en función de los volúmenes prestacionales u otras circunstancias objetivamente atendibles de acuerdo con las actividades a desplegar.

5.- FACTURACIÓN.

La FNMT-RCM realizará una facturación anual con fecha 1 de abril de cada año de vigencia del encargo contra certificación o autorización conformada por la AEPD, y, en su caso, mediante el prorrateo de la cantidad anual a abonar pudiendo, además, liquidar en tales facturas aquellos servicios adicionales o avanzados solicitados. El abono de las facturas se realizará, en un plazo no superior a treinta días de la fecha de factura, mediante transferencia bancaria a la cuenta de la FNMT-RCM:

- Código Cuenta Cliente: 0182-2370-49-0208501334
- IBAN: ES28-0182-2370-4902-0850-1334
- Código BIC: BBVAESMM

Las facturas de la FNMT-RCM se emitirán a nombre de:

- Denominación: Agencia Española de Protección de Datos
- Domicilio: Jorge Juan, 6
- Población: Madrid
- Provincia – CP: 28001
- NIF: Q2813014D
- Departamento o persona de contacto: JEFA DE ÁREA DE GESTIÓN PRESUPUESTARIA Y FINANCIERA
- Teléfono: 91 399 63 25
- Referencia: Dª. María Eugenia Gil Diaz.

6.- SERVICIOS DE VALIDACIÓN (Leyes 39/2015 y 40/2015)

De conformidad con el artículo 24.4 del "REGLAMENTO (UE) nº 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 la que se deroga la Directiva 1999/93/CE",

la puesta a disposición de la información sobre el estado de validez de los certificados reconocidos o cualificados, que emita la FNMT-RCM, no tendrán coste para las Administraciones Públicas.

SÉPTIMA. REVISIÓN Y COMISIÓN DE SEGUIMIENTO

Sin perjuicio de lo dispuesto a efectos de actualización de las condiciones económicas de las actividades encargadas, las partes podrán proponer la revisión de este Encargo en cualquier momento de su vigencia, a efectos de incluir, de mutuo acuerdo, las modificaciones que resulten pertinentes.

A petición de cualesquiera de las partes podrá crearse una comisión mixta para el examen, seguimiento, coordinación del Encargo y, en su caso, adhesiones, así como para plantear propuestas de modificación y de resolución de conflictos.

OCTAVA. RESPONSABILIDAD

La FNMT-RCM como prestador de los servicios citados en la condición primera y Anexos, y la AEPD como destinatario de los servicios de certificación y firma electrónica y encargado de las funciones de registro y acreditación en el procedimiento de identificación, acreditación y registro de los usuarios y, en su caso, administraciones y firmantes/custodios, responderán, cada una en el ámbito de sus respectivas funciones, de los daños y perjuicios que causara el funcionamiento del sistema de acuerdo con las reglas generales del ordenamiento jurídico que resultaran de aplicación y de conformidad con las obligaciones asumidas a través del presente Encargo.

La FNMT-RCM, dado el mandato legal de extensión de los servicios, limita su responsabilidad, siempre que su actuación o la de sus empleados no se deba a dolo o negligencia grave, hasta un importe anual del presente Encargo incrementado en un 10% como máximo.

NOVENA. RESOLUCIÓN Y EXTINCIÓN

Causas de resolución. La FNMT-RCM estará obligada a la realización de las actividades previstas en este Encargo, en su condición de medio propio y servicio técnico, a tenor de lo dispuesto en la legislación citada en este documento, por lo que no podrá instar ninguna de las siguientes causas de resolución sin la autorización previa del órgano directivo de adscripción de la Entidad.

El Encargo podrá resolverse por parte de la AEPD y, en su caso, de los organismos que estén adheridos, cuando existiera manifiesta falta de calidad del servicio, por parte de la FNMT-RCM, o incumplimiento grave de las obligaciones de ésta en el desarrollo de su actividad. La resolución de un organismo adherido o del firmante principal del Encargo, no supondrá la resolución en nombre del resto de organismos que tengan personalidad jurídica independiente de su órgano de adscripción o vinculación.

La FNMT-RCM podrá instar, previa autorización de su órgano de adscripción, la resolución del Encargo por falta de pago del precio acordado, por falta de

consignación presupuestaria / reserva de crédito o por incumplimiento grave de las obligaciones que corresponden a la AEPD.

Causas de extinción.

Serán causas de extinción:

- El cumplimiento del plazo previsto en el Encargo y sus prórrogas.
- El mutuo acuerdo de las partes.

DÉCIMA. PROTECCIÓN DE DATOS

RÉGIMEN

El régimen de protección de datos de carácter personal derivado de este Encargo y de la actuación conjunta de las partes, será el previsto en 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos-RGPD); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y en el Real Decreto 1720/2007, de 21 de diciembre, en lo que no se oponga a las normas antes citadas.

Los ficheros de la FNMT-RCM son de titularidad pública y, anteriormente, se creaban mediante Orden Ministerial (la última, Orden EHA/2357/2008, de 30 de julio, BOE 190, de 7 de agosto). Actualmente, y por aplicación del RGPD y legislación española, la Entidad ha creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos, con el fin de adaptarse al RGPD, que pueden consultarse en: http://www.fnmt.es/rgpd

Los ficheros de la AEPD serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general, de conformidad con la Ley.

Atendiendo al art. 6 letra e) RGPD, el cumplimiento de una misión realizada en interés público, por cuanto que difícilmente puede comprenderse que la base jurídica del tratamiento sea el consentimiento del interesado (bien un funcionario a quien se le emite un certificado digital de firma) en una relaciones con la administración en que necesariamente habrá de contar con una firma digital, y tampoco se considera que la base jurídica pueda ser el interés legítimo de la FNMT, que como entidad pública empresarial dependiente de la Subsecretaría habría de entenderse comprendida dentro del concepto de Administración Pública, y por lo tanto no podría utilizar dicha base jurídica para el tratamiento de los datos personales en virtud de lo establecido en el artículo 6.1, párrafo final, RGPD. Se considera por lo tanto más acertado que la base jurídica de estos tratamientos habrá de ser el interés público o privado de la ley 40/2015 y del artículo 81 de la ley 66/1997 para extender en la mayor medida posible el ámbito de actuación de los certificados digitales, firma electrónica, administración electrónica etc.

COMUNICACIÓN DE DATOS

La comunicación de datos de carácter personal que la AEPD realice a la FNMT-RCM sobre los datos de los empleados públicos de aquélla para la emisión de certificados de firma electrónica en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (y, en su caso, en el del art. 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social), cuenta con el consentimiento del interesado que ha aceptado las condiciones de emisión del certificado al solicitar el mismo y ha sido informado sobre las finalidades del tratamiento de sus datos, sobre los posibles destinatarios y del resto de finalidades e información establecidos en las normas de aplicación (RGPD, art. 13 y LOPDGDD, art. 11), según consta en el Registro de Actividades de Tratamiento:

http://www.fnmt.es/documents/10179/10671624/RAT+06-06-2019/e8afec52-e3cf-90f4-41a3-ff3bdc704ae1 (Tratamiento nº 15).

Todo ello de conformidad con el art. 6.1. del RGPD, existiendo un interés legítimo de la Entidad ya que, además, tal comunicación resulta ineludible para que la FNMT-RCM expida los certificados de firma electrónica a los empleados de la AEPD y, en su caso, a terceros.

ACCESO A LOS DATOS POR CUENTA DE TERCEROS (ENCARGADO DEL TRATAMIENTO)

1) No tendrá carácter de comunicación de datos el acceso que la AEPD, en calidad de Oficina de Registro y Acreditación de la FNMT-RCM, realice sobre los datos de carácter personal que la FNMT-RCM mantiene, como responsable del tratamiento, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del art. 81 de la Ley 66/1997, de 30 de diciembre, descritos en este Encargo. Tales datos son los que figuran en el tratamiento nº 15 del Registro de Actividades de Tratamiento (RAT) de la FNMT-RCM, descrito en el enlace anterior.

2) Por tanto, y de conformidad con el artículo 28 del RGPD, la AEPD actuará en calidad de encargado del tratamiento por cuenta de la FNMT-RCM y asumirá las obligaciones que se establecen en esta condición y en la legislación de aplicación.

3) Las actuaciones concretas que sobre el Tratamiento nº 15 del RAT de la FNMT-RCM que la AEPD realizará sobre los datos serán los siguientes:

☒	Recogida	☒	Registro
☒	Estructuración	☒	Modificación
☒	Conservación	☒	Extracción
☒	Consulta	☐	Comunicación
☐	Difusión	☒	Interconexión
☒	Cotejo	☒	Limitación
☒	Supresión	☐	Destrucción
☐	Otros…	☐	Otros…

4) El encargado del tratamiento, respecto de su actuación en este encargo, se obliga a:

a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso, podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo con las instrucciones del Responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c) Adoptar las medidas de seguridad que exige el Reglamento de desarrollo de la LOPD. Las medidas de seguridad se determinan en función del nivel de seguridad de los ficheros de la FNMT-RCM antes comunicadas y en función del modo y lugar de acceso a los datos personales por los Encargados.

Las medidas de seguridad implantadas para el tratamiento podrán ser objeto de modificación, supresión y/o novación en aras a dar cumplimiento a las exigencias que impone el Reglamento General de Protección de Datos y resto de normativa vigente relacionada. Al efecto se llevará a cabo una evaluación de riesgos, y evaluación de impacto y/o consulta previa, si procediera, en la que se determinará si se precisa implementar otras medidas más adecuadas para garantizar la seguridad del tratamiento, las cuales deberán ser adoptadas, documentando todo lo actuado. En cualquier caso, podrán acordarse aquellas que se establezcan en códigos de conducta, sellos, certificaciones o cualquier norma o estándar internacional actualizado de cumplimiento de protección de datos y seguridad de la información, a que el Responsable o Encargado se hallen adheridos.

Todo el personal al que el encargado proporcione acceso a los datos personales deberá ser informado, de forma expresa, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

d) Llevar por escrito y estar disponible, un Registro Actividades de Tratamiento efectuados por cuenta del responsable, que contenga (en su caso): las transferencias de datos personales a un tercer país u organización internacional,

incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas;

En ese registro, también se incluirá una descripción general de las medidas técnicas, organizativas y de seguridad relativas a:

- La seudonimización y el cifrado de datos personales (en su caso),
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento,
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico y,
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

e) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del tratamiento, en los supuestos legalmente admitidos.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

f) No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado. El Encargado podrá comunicar los datos a otros encargados del tratamiento del mismo responsable, previo consentimiento y de acuerdo con las instrucciones del responsable, indicando los tratamientos que se pretenden subcontratar e identificando, de forma clara e inequívoca, la empresa subcontratista y sus datos de contacto.

En caso de que el Responsable autorice la subcontratación de los servicios por parte del Encargado, éste se compromete a trasladar las obligaciones de este contrato a los subencargados.

g) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el objeto del mismo.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento

3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

k) Si procede, designar un delegado de protección de datos y comunicar su identidad y datos de contacto al Responsable.

l) Devolver al Responsable los datos de carácter personal que hayan sido objeto de tratamiento. En todo caso, el encargado podrá conservar debidamente bloqueados aquellos datos que sean necesarios, en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5) El responsable del tratamiento, respecto de su actuación en este encargo, se obliga a:

a) Facilitar al encargado el acceso a los datos que forman parte de sus ficheros o entregárselos del modo que resulte oportuno para la correcta prestación del servicio.

b) Informar conforme a la normativa a los interesados cuyos datos sean objeto de tratamiento y haber obtenido de los mismos lícitamente su consentimiento expreso o contar con motivos legítimos y acreditables para el mismo.

c) Tener establecida la base legal que legitima el tratamiento.

d) Disponer de mecanismos sencillos para que los interesados puedan ejercitar sus derechos.

e) Contar con análisis de riesgos, con un registro de los tratamientos y evaluaciones de impacto si fuera necesario por la naturaleza de los datos tratados.

f) Tener habilitadas las medidas de seguridad adecuadas para salvaguardar los datos en la transmisión de los datos al Encargado.

g) Nombrar un delegado de protección de datos en los casos que fuera obligatorio y comunicar su identidad al encargado. Actualmente y a la fecha de suscripción del presente contrato los datos del Delegado de Protección de Datos nombrado por la FNMT-RCM son los siguientes:

Delegado de Protección de Datos de la FNMT-RCM
Email: dpd@fnmt.es
Dirección: Calle Jorge Juan 106, CP: 28009 Madrid

En lo no previsto en este documento será de aplicación, en todo caso, la normativa vigente en materia de protección de datos personales.

UNDÉCIMA. RÉGIMEN JURÍDICO Y RESOLUCIÓN DE CONFLICTOS

La prestación de los servicios contemplados en el Encargo y sus Anexos, en cuanto al contenido y características de los mismos, se realizará con sujeción a la regulación contenida en la Ley 59/2003, de 19 de diciembre, de firma electrónica, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social y su normativa de desarrollo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y el resto de disposiciones citadas en el expositivo así como a las disposiciones que sean de aplicación y en su caso, cuantas disposiciones se dictaran, durante la vigencia del Encargo y que afectaran a su objeto.

Este instrumento jurídico formalizado mediante un Encargo a un medio propio personificado es realizado por la AEPD a la FNMT-RCM, de acuerdo con los artículos 6 y 32 de la Ley 9/2017, de 8 de noviembre, con el artículo 3.2 del vigente Estatuto de esta Entidad, aprobado por el Real Decreto 1114/1999, de 25 de junio, y resto de disposiciones que sean de aplicación.

Las partes se comprometen, a través de la comisión prevista en la condición séptima, a resolver de mutuo acuerdo las incidencias que pudieran existir en la interpretación y cumplimiento de este Encargo. Las cuestiones litigiosas que, no obstante, surjan entre las partes se someterán a la Ley 52/1997, de 27 de noviembre, y normas de desarrollo y, en cualquier caso, a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en su Ley reguladora.

DUODÉCIMA. COORDINACIÓN ADMINISTRATIVA

FNMT-RCM procederá a informar de la formalización y, en su caso, extinción de la prestación a que se refiere este Encargo al Ministerio de Hacienda y a la Dirección de Tecnologías de la Información y Comunicaciones, así como a los demás órganos competentes, a los efectos de coordinación e interoperabilidad correspondientes para el desarrollo de la Administración electrónica y el acceso electrónico de los ciudadanos a los Servicios Públicos.

Y, en prueba de conformidad, ambas partes suscriben el presente Encargo y todos sus Anexos, en el lugar indicado en el encabezamiento y en la fecha de las firmas electrónicas.

FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA	**ADMINISTRACIÓN QUE REALIZA EL ENCARGO**
Directora General	***Directora***
Lidia Sánchez Milán	*Mar España Martí*

ANEXO I

CAPITULO I - SERVICIOS EIT

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), como prestador de servicios de certificación, emitirá para todo aquel usuario que lo solicite un conjunto de certificados, denominado "Certificado Básico" o "Título de Usuario", que permite al Titular del mismo comunicarse con otros usuarios, de forma segura.
El formato de los certificados utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de 31 de marzo de 2000 o superiores (ISO/IEC 9594-8 de 2001). El formato será el correspondiente a la Versión 3 del certificado, especificado en esta norma
El certificado será válido para el uso con protocolos de comunicación estándares de mercado, tipo SSL, TLS, etc.
Como servicios de certificación asociados para el uso de los certificados por parte de sus titulares, la FNMT-RCM ofrecerá los siguientes servicios técnicos:

- registro de usuarios
- emisión, revocación y archivo de certificados de clave pública
- publicación de certificados y del Registro de Certificados
- registro de eventos significativos

GENERACIÓN Y GESTIÓN DE CLAVES

Generación y gestión de las claves
En el procedimiento de obtención de certificados, la FNMT-RCM desarrollará los elementos necesarios para activar, en el puesto del solicitante, el software que genere a través de su navegador web, un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.
Las claves privadas serán utilizadas bajo el control del software de navegación web del que disponga el propio usuario, enviando todas las claves públicas a la FNMT-RCM con el fin de integrarlas en un certificado.
Las claves privadas de firma permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por la FNMT-RCM.
La FNMT-RCM garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

Archivo de las claves públicas
Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de 15 años.

Exclusividad de las claves

Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible.

Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

Renovación de claves

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

REGISTRO DE USUARIOS

Registro de usuarios

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el "Certificado Básico" o "Título de Usuario" por la FNMT-RCM.

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogéneo en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta de la FNMT-RCM, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos la FNMT-RCM, dará soporte a la implantación de las distintas oficinas de registro que se establezcan cuando fuere necesario, en los siguientes términos:

a) Aportación de la aplicación informática de registro
b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.
c) Registro y formación de los encargados del registro, lo que supone la emisión de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, incluyendo la firma electrónica de las solicitudes de registro.

Identificación de los solicitantes de los certificados, comprobación de su personalidad y constatación de su voluntad.-

La identificación de los solicitantes de los certificados en las oficinas de registro y la comprobación de su personalidad se hará mediante la exhibición del Documento Nacional de Identidad, Pasaporte u otros medios admitidos en derecho.

En el acto de registro, el personal encargado de las oficinas de acreditación constatará que el solicitante tiene la voluntad de solicitar que le sea emitido un certificado electrónico por la FNMT-RCM y que éste reúne los requisitos exigidos por el ordenamiento jurídico.

En caso de que solicite un certificado de persona jurídica, será de aplicación el procedimiento de verificación de la identidad del solicitante y de comprobación de los datos de constitución de la persona jurídica y de la suficiencia, extensión y vigencia de las facultades de representación del solicitante que se establece en el artículo 13 de la Ley 59/2003, de 19 de diciembre. El detalle del procedimiento figura en la Declaración de Prácticas de Certificación: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Necesidad de presentarse en persona

El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas según el modelo aprobado por la FNMT – RCM para este fin siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

Necesidad de confirmar la identidad de los componentes por la FNMT-RCM

Si se trata de solicitudes relativas a certificados electrónicos a descargar en un servidor u otro componente, la FNMT-RCM requerirá la aportación de la documentación necesaria que le acredite como responsable de dicho componente y, en su caso, la propiedad del nombre del dominio o dirección IP. (Certificado de componente no es un certificado reconocido ni se recoge en la legislación española)

Incorporación de la dirección de correo electrónico del titular al certificado

En su caso, la incorporación de la dirección de correo electrónico del titular al certificado se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.
Cuando la dirección del correo electrónico del titular del certificado conste en una de las extensiones del propio certificado, ni la FNMT–RCM, como firmante y responsable del mismo, ni la AEPD como encargado del registro de usuarios responden de que esta dirección esté vinculada con el titular del certificado.

Obtención del "Certificado Básico" o "Título de usuario"

Para la obtención de este certificado, así como para su revocación o suspensión, el solicitante deberá observar las normas y procedimientos desarrollados a tal fin por la FNMT-RCM de conformidad con la normativa vigente aplicable.

EMISIÓN, REVOCACIÓN Y ARCHIVO DE CERTIFICADOS DE CLAVE PÚBLICA

Emisión de los certificados

La emisión de certificados supone la generación de documentos electrónicos que acreditan la identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada; del mismo modo, la emisión de los certificados implica su posterior envío al directorio de manera que sea accesible por todas las personas interesadas en hacer uso de sus claves públicas.
La emisión de certificados por parte de la FNMT-RCM, sólo puede realizarla ella misma, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos certificados.

La FNMT–RCM, por medio de su firma electrónica, garantizará los certificados, así como la verificación de la identidad y cualesquiera otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, la FNMT-RCM utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.
La FNMT - RCM, una vez emitido el certificado, lo publicará y mantendrá una relación de certificados emitidos durante todo el periodo de vida del mismo en un servicio de acceso telemático, universal, en línea y siempre disponible.
La FNMT-RCM garantiza para un certificado emitido:

a) Que el usuario dispone de la clave privada correspondiente a la clave pública del certificado, en el momento de su emisión.
b) Que la información incluida en el certificado se basa en la información proporcionada por el usuario.
c) Que no omite hechos conocidos que puedan afectar a la fiabilidad del certificado

Aceptación de certificados

✓ Para que un certificado sea publicado por la FNMT-RCM, ésta comprobará previamente:

a) Que el signatario es la persona identificada en el certificado
b) Que el signatario tiene un identificativo único
c) Que el signatario dispone de la clave privada

✓ La AEPD garantizará que, al solicitar un certificado electrónico, su titular acepta que:

a) La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.
b) Únicamente el titular del certificado tiene acceso a su clave privada.
c) Toda la información entregada durante el registro por parte del titular es exacta.
d) El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.
e) El usuario final del certificado no es un Prestador de Servicios de Certificación y no utilizará su clave privada asociada a la clave pública que aparece en el certificado para firmar otros certificados (u otros formatos de certificados de clave pública), o listados de certificados, como un Prestador de Servicios de Certificación o de otra manera.

✓ La AEPD garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

a) A conservar su control.
b) A tomar las precauciones suficientes para prevenir su pérdida, revelación, modificación o uso no autorizado.

Al solicitar el certificado, el titular deberá prestar su conformidad con los términos y condiciones de su régimen y utilización.

Revocación y suspensión de certificados electrónicos

La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, dejará sin efecto los certificados electrónicos otorgados a los usuarios cuando concurra alguna de las siguientes circunstancias:

a) Solicitud de revocación del usuario, por la persona física o jurídica representada por éste o por un tercero autorizado.
b) Resolución judicial o administrativa que lo ordene.
c) Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.
d) Finalización del plazo de vigencia del certificado.
e) Pérdida o inutilización por daños en el soporte del certificado.
f) Utilización indebida por un tercero.
g) Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.
h) Cualquier otra prevista en la normativa vigente.

La extinción de la eficacia de un certificado producirá efectos desde la fecha en que la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda tuviera conocimiento cierto de cualquiera de los hechos determinantes de la extinción previstos en el apartado anterior y así lo haga constar en su Registro de certificados.
En el supuesto de expiración del período de validez del certificado, la extinción surtirá efectos desde que termine el plazo de validez.
La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda podrá suspender temporalmente la eficacia de los certificados si así lo solicita el usuario o lo ordena una autoridad judicial o administrativa, o cuando existan dudas razonables, por parte de cualquier usuario público, sobre la vigencia de los datos declarados y su verificación requiera la presencia física del interesado. En este caso, la FNMT-RCM podrá requerir, de forma motivada, su comparecencia ante la oficina de acreditación donde se realizó la actividad de identificación previa a la obtención del certificado o, excepcionalmente, ante otra oficina de acreditación al efecto de la práctica de las comprobaciones que procedan. El incumplimiento de este requerimiento por un periodo de 10 días podrá dar lugar a la revocación del certificado.
La suspensión de los certificados surtirá efectos en la forma prevista para la extinción de su vigencia.
La extinción de la condición de usuario público se regirá por lo dispuesto en la presente Orden de encargo o lo que se determine, en su caso, por la normativa vigente o por resolución judicial o administrativa.

Comunicación y publicación en el Registro de Certificados de circunstancias determinantes de la suspensión y extinción de la vigencia de un certificado ya expedido.

La FNMT-RCM suministrará a la AEPD los mecanismos de la transmisión segura para el establecimiento de un servicio continuo e ininterrumpido de comunicación entre ambas a fin de que, por medios telemáticos o a través de un centro de atención telefónica a usuarios, se ponga de inmediato en conocimiento de la FNMT-RCM cualquier circunstancia de que tenga conocimiento y que sea determinante para la suspensión, revocación o extinción de la vigencia de los certificados ya expedidos, a fin de que se pueda dar publicidad de este hecho, de manera inmediata, en el directorio actualizado de certificados a que se refiere el artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
La FNMT-RCM pondrá a disposición de los titulares de los certificados un centro de atención de usuarios que permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.

Además, el citado centro de atención a los usuarios permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.
La AEPD y la FNMT-RCM responderán de los daños y perjuicios causados por cualquier dilación que les sea imputable en la comunicación y publicación en el Registro de Certificados, respectivamente, de las circunstancias de que tengan conocimiento y que sean determinantes de la suspensión, revocación o extinción de un certificado expedido.

PUBLICACION DE CERTIFICADOS DE CLAVE PÚBLICA Y REGISTRO DE CERTIFICADOS

-Publicación de certificados de clave pública
La FNMT-RCM publicará los certificados emitidos en un directorio seguro.
Cuando el certificado sea revocado, temporal o definitivamente, este será publicado en el Registro de certificados que incluirá una lista de certificados revocados, comprensiva de los certificados expedidos por la FNMT-RCM cuya vigencia se ha extinguido o suspendido al menos hasta un año después de su fecha de caducidad.
Esta publicación puede ser:

a) Publicación directa por parte de la FNMT-RCM.- Esta operación la realiza la FNMT-RCM a través de la publicación en un directorio propio. La actualización en el directorio seguro de las listas de revocación se realizará de forma continuada.

La consulta de este directorio se realizará en línea, por acceso directo del usuario. Este servicio permite la disponibilidad continua y la integridad de la información almacenada en el directorio. Las listas de revocación serán firmadas con la clave privada de firma de la FNMT-RCM.

b) Publicación en directorios externos.- La FNMT-RCM podrá publicar externamente, en directorios públicos ofrecidos por otras entidades u Organismos, mediante replicación periódica o en línea, tanto certificados como listas de certificados revocados. Estas listas, al igual que las publicadas internamente, irán firmadas con la clave privada de firma de la FNMT-RCM.

Frecuencia de la publicación en directorios externos
La publicación en directorios externos a la FNMT-RCM podrá ser realizada periódicamente o en línea, en función de los requerimientos de la entidad u Organismo que ofrezca el directorio.

Control de acceso
En la publicación directa por parte de la FNMT-RCM, el acceso al directorio se realizará con autenticación previa. Este acceso estará restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.
En cuanto a las listas de revocación, tanto las publicadas interna como externamente, el acceso será público y universal, para verificar este hecho.

REGISTRO DE EVENTOS SIGNIFICATIVOS

Tipos de eventos registrados
La FNMT-RCM registrará todos aquellos eventos relacionados con sus servicios que puedan ser relevantes con el fin de verificar que todos los procedimientos internos

necesarios para el desarrollo de la actividad se desarrollan de acuerdo a la normativa legal aplicable y a lo establecido en el Plan de Seguridad Interna, y permitan detectar las causas de una anomalía detectada.
Todos los eventos registrados son susceptibles de auditarse por medio de una auditoría interna o externa.

Frecuencia y periodo de archivo de un registro de un evento

La frecuencia de realización de las operaciones de registro dependerá de la importancia y características de los eventos registrados (bien sea para salvaguardar la seguridad del sistema o de los procedimientos), garantizando siempre la conservación de todos los datos relevantes para la verificación del correcto funcionamiento de los servicios.
El periodo de archivado de los datos correspondientes a cada registro dependerá asimismo de la importancia de los eventos registrados.

Archivo de un registro de eventos

La FNMT-RCM realizará una grabación segura y constante de todos los eventos relevantes desde el punto de vista de la seguridad y auditoría (operaciones realizadas) que vaya realizando, con el fin de reducir los riesgos de vulneración, mitigar cualquier daño que se produjera por una violación de la seguridad y detectar posibles ataques.
Este archivo está provisto de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación de los certificados y eventos almacenados.
La FNMT-RCM mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a 15 años.
En el caso del archivo histórico de los certificados, éstos permanecerán archivados durante al menos 15 años.

Datos relevantes que serán registrados

Serán registrados los siguientes eventos relevantes:

a) La emisión y revocación y demás eventos relevantes relacionados con los certificados.
b) Todas las operaciones referentes a la firma de los certificados por la FNMT-RCM.
c) Las firmas y demás eventos relevantes relacionados con las Listas de Certificados revocados.
d) Todas las operaciones de acceso al archivo de certificados.
e) Eventos relevantes de la generación de claves.
f) Todas las operaciones del servicio de archivo de claves y del acceso al archivo de claves propias expiradas.
g) Todas las operaciones relacionadas con la recuperación de claves.

Las funciones de administración y operación de los sistemas de archivado y auditoría de eventos serán siempre encomendadas a personal especializado de la FNMT-RCM.

Protección de un registro de actividad

Una vez registrada la actividad de los sistemas, los registros no podrán ser modificados, ni borrados, permaneciendo archivados en las condiciones originales durante el periodo señalado.

Este registro tendrá sólo acceso de lectura, estando restringido a las personas autorizadas por la FNMT-RCM.
La grabación del registro, con el fin de que no pueda ser manipulado ningún dato, se realizará automáticamente por un software específico que a tal efecto la FNMT-RCM estime oportuno.
El registro auditado, además de las medidas de seguridad establecidas en su grabación y posterior verificación, estará protegido de cualquier contingencia, modificación, pérdida y revelación de sus datos durante su grabación en soportes externos, cambio de este soporte y almacenamiento de los mismos.
La FNMT-RCM garantiza la existencia de copias de seguridad de todos los registros auditados.

CAPITULO II - SERVICIOS AVANZADOS

Certificados de componente

La FNMT-RCM emite certificados de componente genérico, de servidor y de firma de código, por lo que se hereda la confianza que representa la FNMT-RCM como Autoridad de Certificación instalada en los navegadores de Microsoft.

- *Certificado SSL/TLS estándar*: es aquel que permite establecer comunicaciones seguras con sus clientes utilizando el protocolo SSL/TLS. Este tipo de certificados garantiza la identidad del dominio donde se encuentra su servicio Web

- *Certificado wildcard*: Identifica todos los sub-dominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos. Por ejemplo, el certificado wildcard emitido a "*.ejemplo.es" garantiza la identidad de dominios como compras.ejemplo.es, ventas.ejemplo.es o altas.ejemplo.es.

- *Certificado SAN*: El certificado de tipo SAN, también conocido como certificado multidominio, UC o Unified Communications Certificates, le permite securizar con un solo certificado hasta doce dominios diferentes.

- *Certificado de sello de entidad* es aquel que se utiliza habitualmente para establecer conexiones seguras entre componentes informáticos genéricos. Su flexible configuración permite dotarle de diferentes usos:

  Autenticación de componentes informáticos de una Entidad en su acceso a servicios informáticos, o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente.
  Intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad.

CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)

Servicio de Validación del Certificado de la AC Administración Pública

Para comprobar la validez del certificado de la Autoridad de Certificación de la Administración Pública, se ha dispuesto dos mecanismos para la descarga de la CRL asociada a dicho certificado. Ambos, se encuentran disponibles en el propio certificado de la AC, como CRLDistributionPoints y son, por este orden:

- **LDAP**

Localización del servicio ldap para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES?authorityRevocationList ?base ?objectclass=cRLDistributionPoint

Este servicio ldap se prestará en su versión 3, en modo binario, estando disponible en el puerto estándar para el servicio ldap (389), y sin requerir ningún tipo de autenticación.

La prestación del servicio será de carácter universal, gratuito, y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada que en este caso solo existe una CRL, la ARL.

El acceso a este servicio estará disponible a través de Internet, así como a través de la Red SARA.

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

- **HTTP**

Localización del servicio http para la descarga de la CRL de la AC RAIZ de la FNMT-RCM:

http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

La CRL emitida para esta infraestructura tendrá un periodo de validez de 3 meses y se publicará 10 días antes de su caducidad y, en cualquier caso, siempre que se revoque algún certificado emitido por la AC RAIZ de la FNMT-RCM.

La prestación del servicio será de carácter universal, gratuito, y sin control de acceso, teniendo únicamente la restricción de poder descargarse una única crl en cada conexión realizada.

El acceso a este servicio estará disponible a través de Internet así como a través de la Red SARA.

La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de Validación de Certificados de Entidad Final para Administración Pública

El servicio de Validación de Certificados para la infraestructura Administración Pública, se prestará mediante los siguientes servicios:

- Servicio de descarga de CRLs de AC Administración Pública mediante protocolo LDAP.
- Servicio de descarga de CRLs de AC Administración Pública mediante protocolo http.

La disponibilidad de múltiples servicios para la validación de certificados proporciona compatibilidad total con las distintas necesidades de las aplicaciones en las que

deberán integrarse los certificados de Entidad Final emitidos por la infraestructura de la Administración Pública.

Servicio de descarga de CRLs mediante protocolo LDAP
Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública.
Este servicio se prestará desde la siguiente URL en el puerto estándar ldap 389:
ldap://ldapape.cert.fnmt.es/CN=CRLnnn,OU=AC APE, O=FNMT-RCM, C=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint
Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado.
El acceso a este servicio estará disponible a través de Internet, así como a través de la Red SARA.
La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

Servicio de descarga de CRLs mediante protocolo HTTP.
Este servicio será de carácter universal, anónimo, gratuito y si ningún tipo de autenticación, de tal forma que cualquier cliente podrá descargarse la CRL para poder validar un certificado de Entidad Final emitido por la AC Administración Pública.
Este servicio se prestará desde la siguiente URL en el puerto estándar http 80:
http://www.cert.fnmt.es/crlsape/CRLnnn.crl
Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de la Administración Pública, siendo en cada caso CRLnnn el número de CRL que le corresponde a dicho certificado al igual que el anteriormente descrito.
El acceso a este servicio estará disponible a través de Internet, así como a través de la Red SARA.
La FNMT-RCM se reserva el derecho a bloquear el acceso a aquellas direcciones IP para las que se observe un uso indebido o abusivo de este servicio.

CERTIFICADO DE FIRMA ELECTRONICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS Y CERTIFICADO DE FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS CON SEUDÓNIMO

Este certificado se emite por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como Prestador Cualificado de Servicios de Confianza.
El certificado para personal al servicio de la Administración Pública es desarrollado por la FNMT-RCM mediante una infraestructura PKI específica y ad hoc, basada en actuaciones de identificación y registro realizadas por la red de Oficinas de Registro designadas por el órgano, organismo o entidad Suscriptora del certificado. Los "Procedimientos de Emisión" podrán establecer, en el ámbito de actuación de las Administraciones Públicas, Oficinas de Registro comunes para este ámbito de

actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.
Son expedidos por la FNMT-RCM como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, citada y en la normativa técnica EESSI, concretamente de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y "ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". Estos certificados electrónicos son emitidos exclusivamente al personal al servicio de la Administración, y por tanto no se emiten al público general.
Los certificados de firma electrónica del personal al servicio de la Administración Pública son cualificados conforme al Reglamento (UE) No 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.
Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl..
El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos es actualmente de 4.096 bits.
El tamaño de las claves RSA relativas a los certificados electrónicos cualificados para identificar a los empleados públicos es actualmente de 2.048 bits.
El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.
FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de la Administración, Organismo o Entidad pública titular correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios, por la propia naturaleza de los certificados de empleado público, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.
Las Administraciones sólo podrán requerir Certificados con seudónimo de firma electrónica del personal al servicio de la Administración Pública y de la Administración de Justicia para su uso en aquellas actuaciones que, realizadas por medios electrónicos, afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización.
El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

Servicio de firma electrónica centralizada para empleados públicos (firma en la nube)

La AC Administración Pública expide certificados de firma electrónica centralizada para funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.
Estos Certificados son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de

conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
El certificado de firma electrónica centralizada para empleados públicos es un certificado cualificado para la creación de firmas electrónicas avanzadas generadas en un dispositivo de creación de firma remoto, en un entorno seguro y confiable. Esto es, la generación de las Claves pública y privada no se realiza directamente en el navegador de Internet del Firmante o en otro dispositivo en su poder, sino que se generan y se almacenan en un entorno seguro perteneciente a la FNMT-RCM. Para proveer este servicio, se ha integrado en la infraestructura de la FNMT-RCM, el módulo TrustedX eIDAS de Safelayer.
El Certificado de firma electrónica centralizada para empleado público, confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, y al suscriptor del certificado, que es el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.
Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del Personal al servicio de la Administración al que se le ha expedido el Certificado. El acceso a las claves privadas del firmante se llevará a cabo garantizando siempre un Nivel de Aseguramiento ALTO (usuario+password + 2º factor de autenticación OTP).
Las funcionalidades y propósitos del Certificado de firma electrónica centralizada para empleado público permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones. La expedición y firma del Certificado se realizará por la "AC Administración Pública" subordinada de la "AC Raíz" de la FNMT-RCM.
Los Certificados de firma electrónica centralizada para empleado público expedidos por la FNMT-RCM tendrán validez durante un periodo máximo de tres (3) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.
La longitud de la clave utilizada en la "AC Administración Pública" es de 2048 bits y en la "AC Raíz" es de 4096 bits.
La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

SELLO ELECTRÓNICO CUALIFICADO DE LAS ADMINISTRACIONES PÚBLICAS

Certificado cualificado de Sello electrónico para Administración Pública, órgano, organismo público o entidad de derecho público, como sistema de identificación y para la actuación administrativa automatizada y para la actuación judicial automatizada, que permite autenticar documentos expedidos por dicha Administración o cualquier activo digital.
Se expiden de conformidad con el estándar europeo ETSI EN 319 411-2 "*Requirements for trust service providers issuing EU qualified certificates*", y ETSI EN 319 412-3 "*Certificate profile for certificates issued to legal persons*".

Los certificados de sello electrónico son cualificados conforme al Reglamento (UE) No 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. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.
La duración de los mismos se establece en 2 años y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.
FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios y custodios de la Administración, Organismo o Entidad pública titular del certificado, propietario o responsable de la unidad administrativa y del componente informático correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados de Sello electrónico de las AA.PP., serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.
El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

CERTIFICADOS CUALIFICADOS DE AUTENTICACIÓN DE SITIOS WEB PARA SEDE ELECTRÓNICA DE LAS ADMINISTRACIONES PÚBLICAS

Certificados para la identificación de sedes electrónicas de la administración pública, organismos y entidades públicas vinculadas o dependientes emitidos por la FNMT – RCM bajo la denominación de certificados administración.
Se expiden de conformidad con el estándar europeo ETSI EN 319 411-2 "*Requirements for trust service providers issuing EU qualified certificates*", y ETSI EN 319 412-4 "*Certificate profile for web site certificates*".
Estos certificados se expiden como cualificados conforme al Reglamento (UE) Nº 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, de conformidad con los estándares europeos ETSI EN 319 411-1 "*Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements*.
Emitidos en conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser fórum.
La duración de los mismos se establece en 2 años y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.
FNMT-RCM no regula el uso de este certificado, dado que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y demás legislación aplicable, limitándose a crear una infraestructura técnica a disposición de los usuarios

y custodios de la Administración, Organismo o Entidad pública titular de la Sede electrónica correspondiente. Asimismo, todas aquellas circunstancias y requisitos referentes a los usuarios y custodios, por la propia naturaleza de los certificados para la identificación de Sedes electrónicas, serán controlados, exclusivamente, por la Administración, informando a la FNMT-RCM de su alteración o modificación; todo ello, a través a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

El perfil del certificado es el descrito en las declaraciones de prácticas de certificación.

Nota sobre prestación de los servicios

Los servicios contemplados en el presente Anexo I, que preste la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, se realizarán de conformidad con lo establecido en la legislación aplicable a los mismos y los acuerdos, encomiendas, convenios o contratos que suscriba la FNMT-RCM con las diferentes administraciones públicas o con personas o entidades privadas.

ANEXO II
CAPITULO I - SERVICIOS EIT

1. Tarifa anual de los servicios

Se establece una tarifa fija para los servicios EIT, en caso de ser solicitada su activación de forma expresa por parte de la AEPD, de 1.000 Euros al año, impuestos no incluidos.

2. Soporte Técnico

El coste del soporte técnico realizado por parte de personal de la FNMT-RCM será de 122,64 Euros/hora.
En el caso en que el soporte técnico se preste en las instalaciones del conviniente, a la tarifa anterior le serán añadidos los gastos derivados de la estancia fijados en 204,38 Euros/día por persona, más los derivados del desplazamiento y pernocta.

3. Réplica de Directorio para los servicios EIT

Se establece un precio de 20.539,66 €/año por la réplica diaria de las listas de certificados revocados desde la FNMT-RCM a las instalaciones del conviniente por redes públicas. Este precio incluye la licencia de uso del directorio X.500 InJoin Directory Server de Critical Path en las propias instalaciones del cliente.

Este servicio no incluye la instalación ni el mantenimiento, que serán por cuenta del conviniente.
El directorio y su contenido no podrá ser cedido a terceros bajo ningún concepto, y deberá ser protegido contra todo acceso por entidades ajenas al conviniente, incluyendo el acceso de consulta.

4. Condiciones

A todas las cantidades expuestas en este capítulo I se les añadirá el IVA legalmente establecido.

CAPITULO II - SERVICIOS AVANZADOS

1. Certificados de componente

El precio anual establecido en el apartado 1 del Capítulo I del presente Anexo de Precios incluye un número máximo de 5 certificados de componente.
El precio de los certificados adicionales será el estipulado en el apartado correspondiente de la página web de Ceres:
www.cert.fnmt.es/catalogo-de-servicios/certificados-electronicos

2. Condiciones

A todas las cantidades expuestas en el presente capítulo II habrá que añadirlas el IVA legalmente establecido.

CAPITULO III - SERVICIOS ADMINISTRACIÓN PÚBLICA (LEY 40/2015)

1. Certificados para los servicios del ámbito de la Ley 40/2015

El precio anual para los servicios del ámbito de la Ley 40/2015 asciende a 6.500,00 Euros/año impuestos no incluidos, incluye la emisión de todos certificados de empleado público que el conviniente requiera, 1 certificado de sede electrónica y 3 certificados de sello electrónico.

2. Condiciones

A todas las cantidades expuestas en el capítulo III del presente Anexo habrá que añadirlas el IVA legalmente establecido.