III. OTRAS DISPOSICIONES

CORTES GENERALES

11243 *Resolución de 12 de mayo de 2026, del Congreso de los Diputados, por la que se publica el Convenio con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, E.P.E., M.P., por el que se encomienda la gestión para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios electrónicos, informáticos y telemáticos en el ámbito de actuación del Congreso de los Diputados.*

La Mesa del Congreso de los Diputados, en su reunión del día 21 de abril de 2026, autorizó la formalización del Convenio entre el Congreso de los Diputados y la «Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, entidad pública empresarial, medio propio», por el que se encomienda la gestión para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en el ámbito de actuación del Congreso de los Diputados.

Al amparo de dicho acuerdo, con fecha 30 de abril de 2026, el Secretario General del Congreso de los Diputados y la Directora General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) han suscrito dicho convenio que figura como anexo.

De conformidad con lo previsto en el artículo 11.b) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y para general conocimiento, se dispone la publicación de dicho convenio anexo a la presente resolución, la cual se emite por el Secretario General del Congreso de los Diputados, actuando en nombre y representación del Congreso de los Diputados, en virtud del nombramiento de la Mesa de la Cámara de 3 de noviembre de 2023 («Boletín Oficial de las Cortes Generales», Sección Cortes Generales, serie B: Régimen Interior, núm. 7, de 4 de noviembre de 2023).

Palacio del Congreso de los Diputados, 12 de mayo de 2026.–El Secretario General del Congreso de los Diputados, Fernando Galindo Elola-Olaso.

ANEXO

Convenio entre el Congreso de los Diputados y la «Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio», por el que se encomienda la gestión de garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en el ámbito de actuación del Congreso de los Diputados

En Madrid, a fecha de firma electrónica.

REUNIDOS

De una parte, don Fernando Galindo Elola-Olaso en calidad de Secretario General del Congreso de los Diputados, en virtud de nombramiento de la Cámara de 3 de noviembre de 2023 («Boletín Oficial de las Cortes Generales», Sección Cortes Generales, serie B: Régimen Interior, núm. 7, de 4 de noviembre de 2023), actuando en nombre y representación del Congreso de los Diputados.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Y, de otra parte, doña María Isabel Valldecabres Ortiz, Directora General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio (en adelante, FNMT-RCM, E.P.E., M.P.), nombrada por Real Decreto 726/2021, de 3 de agosto (BOE núm. 185, de 4 de agosto), en nombre y representación de esta entidad, según el artículo 18 de su estatuto, con domicilio institucional en Madrid, calle Jorge Juan, 106, y NIF Q2826004J.

La FNMT-RCM, E.P.E., M.P., está regulada por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante LRJSP) y por su estatuto, aprobado por Real Decreto 51/2023, de 31 de enero (BOE núm. 27, de 1 de febrero de 2023); encontrándose adscrita al Ministerio de Hacienda, a través de la Subsecretaría de Hacienda, en virtud del artículo 12.11.b) del Real Decreto 206/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda.

Ambas partes, reconociéndose respectivamente capacidad legal y competencia suficientes para formalizar el presente convenio

EXPONEN

Primero.

Que el Congreso de los Diputados, es un órgano constitucional independiente, dotado de la autonomía necesaria para libre ejercicio de sus funciones constitucionales.

El Congreso de los Diputados está interesado en continuar impulsando la implantación de las herramientas en el ámbito de la Administración electrónica, fin común al que persigue la FNMT-RCM, E.P.E., M.P., cuyos medios técnicos son idóneos para conferir seguridad a las comunicaciones telemáticas que envíe y reciba el Congreso de los Diputados, y a los documentos que produzca, en desarrollo de los fines que legalmente tiene atribuidos.

La Mesa del Congreso de los Diputados, en su reunión de 21 de abril de 2026, acordó autorizar la formalización del presente convenio.

Segundo.

El artículo 4.1.g) del Estatuto de la FNMT-RCM, E.P.E., M.P., reconoce y establece, como una de sus funciones y competencias (fijadas por el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social), la prestación de servicios de seguridad en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), así como los servicios de identificación electrónica y de confianza para las transacciones electrónicas, dirección electrónica habilitada y notificación electrónica, digitalización, depósito y custodia de documentos en cualquier soporte, y la expedición, fabricación y suministro de los títulos o certificados de usuario, en soporte digital o en tarjeta; la provisión de servicios *blockchain* y de emisión y verificación de credenciales descentralizadas, y el desarrollo y prestación de servicios digitales para la transformación digital de las Administraciones públicas, de acuerdo con los términos que establezcan las disposiciones legales de ámbito nacional, comunitario o internacional, actividades reguladas actualmente, entre otros, por el Reglamento UE núm. 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 (en adelante, Reglamento (UE) núm. 910/2014).

En el ámbito de identificación electrónica de los interesados en un procedimiento, los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPAC), establecen que, entre otros sistemas utilizados por los interesados y admitidos por las Administraciones públicas «los interesados podrán identificarse electrónicamente (…) Sistemas basados

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

Esta lista de confianza se elabora según lo previsto en la Decisión de Ejecución (UE) 2015/1505, de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza. La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) es uno de los prestadores de servicios de certificación incluidos en esta Lista de confianza gestionada por el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial-SGAD).

https://avancedigital.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

Por otro lado, la LRJSP, establece el funcionamiento electrónico del sector público siendo lo habitual la utilización de los medios electrónicos por las Administraciones públicas, 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 LRJSP, 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.

El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, desarrolla y concreta las previsiones legales, antes esbozadas, con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La Agenda España Digital 2026 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público (eje 5), cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos. Además, en el año 2026 se han añadido, a los diez ejes estratégicos originales, dos ejes transversales para impulsar proyectos estratégicos de gran impacto a través de la colaboración público-privada y la cogobernanza del Estado y las comunidades autónomas.

Tercero.

El Reglamento (UE) núm. 910/2014, para garantizar el correcto funcionamiento del mercado interior y aspirar alcanzar un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza, establece: (a) las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica; (b) las normas para los servicios de confianza, en particular para las transacciones electrónicas, y (c) un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

En el ámbito del derecho interno sobre esta materia, directamente vinculada con el Reglamento (UE) núm. 910/2014, se ha aprobado la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante Ley 6/2020, de 11 de noviembre). La función de esta ley es complementar al Reglamento europeo en aquellos aspectos concretos que no han sido armonizados y cuyo desarrollo se prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

En relación con la actividad y efectos de los sistemas de identificación y demás servicios, la disposición adicional segunda de la Ley 6/2020, de 11 de noviembre, establece que todos los sistemas de identificación, firma y sello electrónico previstos en la LPAC, y en la LRJSP, tendrán plenos efectos jurídicos, entre ellos los sistemas proporcionados por la FNMT-RCM, E.P.E., M.P.

Cuarto.

El artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, bajo el título «Prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre para las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos», faculta a la FNMT-RCM, E.P.E., M.P., para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (apartado 1.º), y le habilita, tras la modificación operada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, previa formalización del correspondiente convenio (u otro instrumento de relaciones), a prestar a las personas, entidades y corporaciones que ejerzan funciones públicas los citados servicios y a su participación en los trámites de identificación y registro.

Tal artículo, 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 se establece en los artículos 17, 26 y 27 de la LPAC y en la LRJSP.

En relación con las actividades de identificación y registro, la FNMT-RCM, E.P.E., M.P., conforme a lo dispuesto en el apartado Nueve del citado artículo 81, podrá celebrar convenios que se consideren adecuados 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.

El Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el reiterado artículo 81, regula el régimen de prestación de servicios de seguridad por la FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., para establecer los términos que deben regir la prestación de sus servicios en relación con las comunicaciones empleando técnicas y medios electrónicos, informáticos y telemáticos, así como la colaboración mutua en materia de registro y acreditación (tanto de los interesados como de la propia institución y sus empleados).

La FNMT-RCM, E.P.E., M.P., desde mediados de los años noventa, ha desarrollado, mejorado y actualizado diversas infraestructuras de clave pública (PKI), que cubren las necesidades de la LPAC, y LRJSP, soluciones que son potencialmente extensibles a otras Administraciones públicas, Entes, Entidades y resto de órganos y poderes del Estado. Estas PKI se han puesto en marcha obedeciendo a los siguientes criterios:

– Aprovechamiento de la experiencia acumulada en el proyecto de Certificación Española CERES, que constituye el núcleo de la infraestructura de clave pública.
– Reducción de riesgos en la consolidación de la «Administración sin papeles».

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

– Economía de medios, derivada de la experiencia acumulada y transferencia de tecnologías entre Administraciones públicas.

– Reutilización de tecnologías, equipamientos, tarjetas y aplicaciones actualmente en uso.

Quinto.

El artículo 11 de la LRJSP, dispone que la realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño. Por medio del presente instrumento, se pretende encomendar a la FNMT-RCM, E.P.E., M.P., la realización de las actividades necesarias para el cumplimiento de los fines del encomendante.

Dado que es de interés del Congreso de los Diputados garantizar que los interesados puedan relacionarse a través de medios electrónicos, así como poder identificarse y establecer comunicaciones con los interesados y otras administraciones, y que la FNMT-RCM, E.P.E., M.P., está en disposición de realizar las actividades técnicas y de seguridad relativas a la certificación, firma electrónica y resto de actuaciones previstas en este documento, según sus fines institucionales; se establece por el Congreso de los Diputados encomendar a la FNMT-RCM, E.P.E., M.P., su realización sobre la base de las siguientes

CLÁUSULAS

Primera. *Objeto.*

Constituye la finalidad de este convenio la encomienda de gestión del Congreso de los Diputados a la FNMT-RCM, E.P.E., M.P., para la prestación de actividades de carácter material, técnico y de seguridad necesarias 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 en la actividad que constituye el objeto del Congreso de los Diputados, con sujeción al régimen jurídico y a las condiciones técnicas que se estipulan en las cláusulas siguientes. En particular la FNMT-RCM, E.P.E., M.P., llevará a cabo las actividades en los términos que refleja el anexo I de este convenio.

PACK SP:

Certificados de empleada/o público ilimitado.
Sede electrónica S.P.
Sello electrónico S.P.s.
Dos (2) certificados de componente (SSL o sello).
Sellado de tiempo.

Para la JEC:

Un (1) certificado adicional de sello electrónico.
Un (1) certificado adicional de sede electrónica.

Segunda. *Ámbito subjetivo de aplicación.*

Dentro del ámbito de aplicación subjetivo de este convenio de encomienda de gestión, se encuentra el Congreso de los Diputados y la Junta Electoral Central (JEC).

La FNMT-RCM, E.P.E., M.P., podrá extender el ámbito de aplicación de la presente encomienda a las personas que tengan la condición de usuarios de acuerdo con la

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

normativa vigente y las cláusulas de este convenio de encomienda de gestión cuando los usuarios se relacionen con el Congreso de los Diputados en el marco de su objeto social.

A tal efecto el Congreso de los Diputados asume que los certificados que expida la FNMT-RCM, E.P.E., M.P., son universales y que por tanto servirán para las relaciones jurídicas que al efecto mantengan sus titulares con las diferentes Administraciones públicas y demás personas y entidades públicas y privadas.

Tercera. *Oficina de registro.*

A efectos de este convenio de encomienda de gestión, el Congreso de los Diputados, tendrá la consideración de Oficina de Registro de la FNMT-RCM, E.P.E., M.P.

Cuarta. *Actividades a desarrollar.*

De acuerdo con el régimen de competencias y funciones propias de cada parte, corresponde a la FNMT-RCM, E.P.E., M.P., en función de lo dispuesto en el objeto de este convenio de encomienda de gestión y en la normativa referida en el mismo, la puesta a disposición al Congreso de los Diputados, de la Plataforma Pública de Certificación desarrollada para el funcionamiento de la Administración electrónica, para ofrecer seguridad en la utilización de instrumentos de identificación electrónica por parte de los interesados y de las administraciones y otros entes del Estado. Estas Plataformas, junto con otras funcionalidades adicionales, como el Sellado de Tiempo, permiten, a la FNMT-RCM, E.P.E., M.P., la realización de las actividades de carácter material y técnico en el ámbito de la securización de las comunicaciones, de la certificación y firma electrónica, cumpliendo con su mandato de extensión de la Administración electrónica.

De otra parte, corresponde al Congreso de los Diputados la realización de las actuaciones administrativas y el desarrollo de sus funciones y competencias dirigidas a la implementación de las Plataformas en sus procedimientos. Para la adecuada consecución del objeto de este convenio de encomienda de gestión, las partes han de desplegar una serie de actuaciones:

1. La FNMT-RCM, E.P.E., M.P., realizará las siguientes actividades:

1. Aportar la infraestructura técnica, organizativa y de seguridad relacionada en el anexo I de este convenio de encomienda de gestión y de conformidad con el estado de la técnica.

2. Aportar los derechos de propiedad industrial e intelectual necesarios, garantizando su uso pacífico. La FNMT-RCM, E.P.E., M.P., excluye cualesquiera licencias o sublicencias, a terceras partes o a la Entidad encomendante para aplicaciones y sistemas de la Entidad encomendante, o de terceros, distintas de las aportadas directamente por la FNMT-RCM, E.P.E., M.P., en virtud de este convenio de encomienda de gestión.

3. Prestar la asistencia técnica que se precise con objeto de facilitar a la Entidad encomendante la información necesaria para el buen funcionamiento de los sistemas, de conformidad con lo establecido en el anexo I de este convenio de encomienda de gestión y, en especial, al despliegue del Registro de Usuarios que se describe en el capítulo I:

– Suministrar procedimientos de activación de una RA.
– Formación específica para el desempeño de las funciones de operador de RA.
– Acceso autenticado a la aplicación de Registro de la FNMT-RCM.
– Supervisión y auditoría de las buenas prácticas de funcionamiento de la RA.
– Soporte especializado y directo a incidencias en la actividad de registro.
– Soporte especializado y directo en la solicitud de certificados de componente.
– Suministro de información estadística de la actividad realizada por su RA.

4. Actualizar tecnológicamente los sistemas, de acuerdo con el estado de la técnica, las disponibilidades presupuestarias de la FNMT-RCM, E.P.E., M.P., y los Esquemas Nacionales de Interoperabilidad y Seguridad, sin perjuicio de la aprobación de

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

los requisitos técnicos correspondientes por la Comisión de Estrategia TIC o, en su caso, por el órgano competente.

5. Aportar la tecnología necesaria para que las obligaciones de la Entidad encomendante, 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.

6. Tener disponible para consulta de la Entidad encomendante y de los usuarios una Declaración de Prácticas de Certificación (DPC), que contendrá, al menos, las especificaciones establecidas en el Reglamento (UE) 910/2014 y en la Ley 6/2020, de 11 de noviembre. Esta DPC, podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, E.P.E., M.P., 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. La DPC y demás información de interés, estará disponible en la dirección electrónica (URL) siguiente:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

La FNMT-RCM, E.P.E., M.P., se compromete, en el desarrollo y ejecución del convenio de encomienda de gestión 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.

De desarrollo de las facultades establecidas en su normativa específica, realizando su actividad en los términos y con los efectos previstos en el Real Decreto 1317/2001, de 30 de noviembre, en especial:

– Funciones de comprobación, coordinación y control de las Oficinas de Registro y Acreditación, sin perjuicio de su dependencia, orgánica y funcional, de la Administración u organismo público a que pertenezcan.

– Resolución de los recursos y reclamaciones de competencia de la FNMT-RCM, E.P.E., M.P., derivadas de la actividad convenida.

– Comunicación al Ministerio de Hacienda a los efectos de coordinación e interoperabilidad correspondientes para el desarrollo de la Administración electrónica y Acceso electrónicos de los ciudadanos a los servicios públicos.

2. El Congreso de los Diputados para una adecuada funcionalidad de los sistemas, realizará las siguientes actuaciones:

1. Designar a un Responsable de Operaciones de Registro (ROR) como representante del Congreso de los Diputados, e interlocutor máximo del mismo con la FNMT-RCM., E.P.E., M.P., y responsable de la supervisión permanentemente de la seguridad y los procedimientos de actuación de los registradores que operen las oficinas de Registro.

2. 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. Todo ello, a través de la Oficina de Registro y acreditación designada ante la FNMT-RCM, E.P.E., M.P., utilizando los procedimientos establecidos por esta Entidad, que figuran en la aplicación de Registro (aplicación web) y en la DPC de la FNMT-RCM, E.P.E., M.P., Tales procedimientos, son documentos sujetos a verificaciones y auditorías por lo que podrán ser modificados por la FNMT-RCM, E.P.E., M.P., a los efectos de mejorar el servicio.

https://www.sede.fnmt.gob.es/registro-inicio

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

El Congreso de los Diputados se compromete, en el desarrollo y ejecución del presente convenio de encomienda de gestión, 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. Régimen de las Oficinas de Registro y Acreditación:

General: 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 facilitado por el Congreso de los Diputados. Cualquier modificación o alteración de dicha relación o de la ubicación de las Oficinas deberá ser comunicada a la FNMT-RCM, E.P.E., M.P.

Las aplicaciones informáticas necesarias para llevar a cabo las actividades de acreditación e identificación serán facilitadas por la FNMT-RCM, E.P.E., M.P., 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 establecidos por la FNMT-RCM, E.P.E., M.P., y a la Declaración de Prácticas de Certificación de la Entidad accesible como en la dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

– Para actuaciones en el ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social: El Congreso de los Diputados, dispondrá de Oficina u Oficinas de Registro y Acreditación que deberán contar con los medios informáticos y sistemas de seguridad precisos para conectarse telemáticamente con la FNMT-RCM, E.P.E., M.P., En ellas, la acreditación e identificación de los solicitantes de los certificados (ciudadanos y empresas, con o sin personalidad jurídica) 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, verificándose de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Las acreditaciones realizadas surtirán plenos efectos y serán válidas para su aceptación por cualquier Administración Pública u otra entidad que admita los certificados emitidos por la FNMT-RCM, E.P.E., M.P.

– Para actuaciones en el ámbito de la LRJSP: Las Oficinas de Registro del Congreso de los Diputados dependerán orgánica y funcionalmente de él (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, E.P.E., M.P., en su condición de Prestador de Servicios de Confianza) y determinarán la identidad y competencia del propio Congreso de los Diputados y la de los diferentes usuarios (firmantes/custodios) designados por la Administración titular de los certificados, de conformidad con la DPC General y las Políticas y Prácticas de Certificación Particulares de Administración Pública, disponibles para consulta en la web: https://www.sede.fnmt.gob.es/dpcs/acap, correspondientes a los certificados y sistemas de firma electrónica de este ámbito de aplicación y con los formularios y condiciones de utilización de cada tipo de certificado.

A tal efecto, el Congreso de los Diputados podrá disponer de las Oficinas de Registro y Acreditación que considere necesarias para la acreditación de este tipo de certificados, deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM, E.P.E., M.P., y realizar las solicitudes de emisión de los certificados. En estas Oficinas de Registro, donde se acreditarán e identificarán 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.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Quinta. *Financiación.*

Las partes de este convenio de encomienda de gestión asumirán, cada una, los costes por la actividad desplegada en el mismo de acuerdo con sus competencias. No obstante, el Congreso de los Diputados asume la obligación de financiar las actuaciones específicas desarrolladas por la FNMT-RCM, E.P.E., M.P., en el marco competencial de actuación de la Administración encomendante, teniendo en cuenta que la actividad de la FNMT-RCM, E.P.E., M.P., está orientadas a costes y su régimen se establece en el Estatuto de la Entidad y en las disposiciones legales que le sean de aplicación.

1. Reembolso de gastos por la realización de actividades en materia de certificación electrónica.

La FNMT-RCM, E.P.E., M.P., como compensación por las actividades, de carácter material o técnico, percibirá, en las anualidades 2026, 2027 y 2028 la cantidad de dos mil quinientos diez euros (2.510,00 euros) y en la anualidad 2029 la cantidad de dos mil novecientos euros (2.900,00 euros), IVA excluido. En caso de que el período inicial de duración del convenio de encomienda de gestión sea inferior a un (1) año, la cantidad anterior se prorrateará, reduciéndose proporcionalmente.

Si hubiera petición expresa, por parte del Congreso de los Diputados de extensión de otras actividades o funcionalidades, entre las recogidas en el anexo I, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de los importes reflejados en el anexo II, del presente convenio de encomienda de gestión.

2. Reembolso en años sucesivos.

En caso de prórroga del convenio de encomienda de gestión, se aplicará el mismo criterio en función de las compensaciones a percibir, actividades solicitadas y duración de las prórrogas.

3. Facturación.

La financiación de las actividades técnicas realizadas por la FNMT-RCM, E.P.E., M.P. (que incluirá, en su caso, las actuaciones adicionales solicitadas), se efectuará de forma anual. El presente convenio de encomienda de gestión tendrá una duración de cuatro años, entrando en vigor en el día de su firma, sin perjuicio de las prórrogas que, por acuerdo expreso entre las partes puedan acordarse.

El régimen de pagos se realizará con periodicidad anual, devengándose cada anualidad desde la fecha de su entrada en vigor. El primer pago deberá efectuarse en el momento de la firma, correspondiendo la anualidad inicial computada desde dicha fecha; los pagos sucesivos se realizarán al inicio de cada anualidad en la forma que se determina a continuación.

El abono de las facturas se realizará, en un plazo no superior a treinta (30) días de la fecha de factura, mediante transferencia bancaria a la cuenta de la FNMT-RCM, E.P.E., M.P.:

– CCC: 0182 2370 49 0208501334.
– IBAN: ES28 0182 2370 4902 0850 1334.
– Código BIC: BBVAESMM.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Las facturas de la FNMT-RCM, E.P.E., M.P. se emitirán a nombre de:

Denominación: Congreso de los Diputados.
Calle: Floridablanca, s/n.
Población: Madrid.
Provincia: Madrid.
NIF: S2804002J.
Departamento o persona de contacto: Departamento de Gestión Dirección de TIC (gestion.tic@congreso.es).
Datos para facturación electrónica (en su caso):

Sexta. *Plazo de duración.*

Este convenio de encomienda de gestión entrará en vigor el día de su firma, y su duración se extenderá durante cuatro (4) años, dejando sin efecto el convenio actualmente en vigor y la posterior adenda asociada al mismo.

Si se mantuviera la necesidad de realización de las actividades de carácter material o técnico por parte de la FNMT-RCM, E.P.E., M.P., el Congreso de los Diputados podrá acordar su prórroga por el periodo anual hasta un máximo de cuatro (4) años, que será asumida por la FNMT-RCM, E.P.E., M.P., siempre que cuente con los recursos suficientes y de conformidad con la ley. Si la prórroga inicial tuviera una duración inferior a cuatro (4) años, podrán acordarse sucesivas prórrogas hasta alcanzar el plazo máximo de cuatro (4) años del presente convenio de encomienda de gestión.

Para materializar las prórrogas, antes del vencimiento inicial del convenio de encomienda de gestión, o el de sus prórrogas, ambas partes suscribirán una adenda que establezca la duración de cada prórroga y, en su caso, sus condiciones.

Séptima. *Revisión.*

Las partes podrán proponer la revisión o actualización del convenio de encomienda de gestión en cualquier momento de su vigencia, a efectos de incluir las modificaciones que resulten pertinentes.

Octava. *Responsabilidad.*

La FNMT-RCM, E.P.E., M.P., como prestador de las actividades descritas en el presente convenio de encomienda de gestión, y el Congreso de los Diputados como destinatario de las mismas y encargado de las funciones incluidas en el procedimiento de identificación, acreditación y registro de los usuarios y, en su caso, de las 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 convenio de encomienda de gestión.

La FNMT-RCM, E.P.E., M.P., dado el mandato legal de extensión de estos servicios y actividades, limita su responsabilidad, siempre que su actuación o la de sus empleados no se deba a dolo o negligencia grave, hasta un importe anual de este convenio de encomienda de gestión incrementado en un diez por ciento (10%) como máximo.

Novena. *Resolución y extinción.*

Causas de resolución

La FNMT-RCM, E.P.E., M.P., estará obligada a la realización de las actividades previstas en este convenio de encomienda de gestión, a tenor de lo dispuesto en la legislación citada en este documento, por tanto, el convenio de encomienda de gestión podrá resolverse, por parte del Congreso de los Diputados, cuando existiera manifiesta

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

falta de calidad en la realización de las actividades, por parte de la FNMT-RCM, E.P.E., M.P., o incumplimiento grave de las obligaciones de esta en el desarrollo de su actuación.

La FNMT-RCM, E.P.E., M.P., podrá instar la resolución del convenio de encomienda de gestión por falta de pago del precio acordado, por falta de consignación presupuestaria/reserva de crédito o por incumplimiento grave de las obligaciones que corresponden al Congreso de los Diputados.

Causas de extinción

Serán causas de extinción:

– El cumplimiento del plazo previsto en este documento y, en su caso, sus prórrogas.
– El mutuo acuerdo de las partes.

Décima. *Protección de datos.*

Las Partes manifiestan que se someten de forma expresa a la normativa vigente en materia de Protección de Datos de Carácter Personal, comprometiéndose a dar un uso debido a los datos de tal naturaleza a los que pudieran, recíprocamente, acceder como consecuencia del desarrollo del presente convenio de encomienda de gestión.

Régimen

El régimen de protección de datos de carácter personal derivado de este convenio de encomienda de gestión 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 resto de normativa relacionada en vigor.

La FNMT-RCM, E.P.E., M.P., 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 https://www.fnmt.es/politica-privacidad.

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

El Congreso de los Diputados ha creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos, con el fin de adaptarse al RGPD.

Delegado de Protección de Datos del Congreso de los Diputados.
Email: dpd@congreso.es.
Dirección: Plaza de las Cortes, núm. 1, 28014 Madrid.

Comunicación de datos

La comunicación de datos de carácter personal que el Congreso de los Diputados realice a la FNMT-RCM, E.P.E., M.P., sobre los datos de los empleados públicos de aquélla para la emisión de certificados de firma electrónica en el ámbito de la LRJSP(y, en su caso, en el del artículo 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

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

de aplicación (RGPD, artículo 13 y LOPDGDD, artículo 11), según consta en el Registro de Actividades de Tratamiento antes señalado (Tratamiento n.º 13 – Gestión de la PKI).

Todo ello de conformidad con el artículo 6.1.c) del RGPD, existiendo un cumplimiento legal aplicable a la Entidad ya que, además, tal comunicación resulta ineludible para que la FNMT-RCM, E.P.E., M.P., expida los certificados de firma electrónica a los empleados de Congreso de los Diputados y, en su caso, a terceros.

Acceso a los datos por cuenta de terceros (encargado del tratamiento)

En términos generales y de conformidad con el artículo 11.2 de la LRJSP, la FNMT-RCM, E.P.E., M.P., como entidad encomendada tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución del convenio de encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal.

De manera específica, dados los mecanismos de gestión de la Plataforma de Registro y Acreditación, el encomendante también tendrá carácter de encargado del tratamiento en relación con el de acceso a datos personales si actuara como Oficina de Registro y Acreditación, por cuenta de la FNMT-RCM, E.P.E., M.P., de conformidad con los siguientes criterios y condiciones:

1) No tendrá carácter de comunicación de datos el acceso que el Congreso de los Diputados, en calidad de Oficina de Registro y Acreditación de la FNMT-RCM, realice sobre los datos de carácter personal que la FNMT-RCM, E.P.E., M.P., mantiene, como Responsable del tratamiento, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, descritos en este documento. Tales datos son los que figuran en el tratamiento n.º 13 del Registro de Actividades de Tratamiento (RAT) de la FNMT-RCM, E.P.E., M.P., descrito en el enlace anterior.

2) Por tanto, y de conformidad con el artículo 28 del RGPD, el Congreso de los Diputados actuará en calidad de Encargado del tratamiento por cuenta de la FNMT-RCM, E.P.E., M.P., y asumirá las obligaciones que se establecen en esta condición y en la legislación de aplicación.

3) Las actuaciones concretas que sobre el Tratamiento núm. 13 del RAT de la FNMT-RCM, E.P.E., M.P., que el Congreso de los Diputados 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 convenio de encomienda de gestión, se obliga a:

a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, solo para la finalidad objeto de este convenio de encomienda de gestión. 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

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

Adoptar las medidas de seguridad que exige el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad). Las medidas de seguridad se determinan en función del nivel de seguridad requerido por el tratamiento y el tipo de datos, así como del modo y lugar de acceso a los datos personales por los Responsables y Encargados. También se tendrán en cuenta las instrucciones de la AEPD.

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.

c) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga: las transferencias de datos personales a un tercer país u organización internacional (en su caso), 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 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.

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admitidos, especificando qué datos se pueden se pueden ceder y cuáles no.

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.

e) 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.

El encargado se compromete a informar al responsable de la existencia de subencargados, tanto al inicio de la contratación como si se produjese de forma sobrevenida durante la ejecución de la misma. El responsable podrá oponerse a la subcontratación. Quedan exceptuados los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

En caso de que el responsable autorice la subcontratación de los servicios por parte del encargado, este se compromete a trasladar las obligaciones de este contrato a los subencargados. Cualquier cambio o modificación sobre los subencargados también deberá de ser notificada al responsable.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

f) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente convenio de encomienda de gestión, incluso después de que finalice el objeto de la misma.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

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 individuales automatizadas (incluida la elaboración de perfiles).

k) Contribuir a las auditorías que realice el responsable del tratamiento o que le realicen por requerimiento de terceros legitimados.

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

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

n) Exonerar al Responsable de cualquier responsabilidad que se pudiera generar por el incumplimiento por parte de los encargados del tratamiento de las estipulaciones del presente convenio de encomienda de gestión.

5) El Responsable del tratamiento, respecto de su actuación en este convenio de encomienda de gestión, 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) En el caso de que el Encargado tenga entre sus opciones la transferencia de datos personales a otras jurisdicciones fuera del Espacio Comunitario (UE) deberá de informar al Responsable de esta circunstancia, teniendo este la capacidad de objetar sobre dichas transferencias o, en su caso, resolver el contrato en el caso de que pudiesen afectarle.

El Encargado deberá también informar al Responsable sobre cualquier transferencia de datos que le pudiese afectar sobre sus proveedores, otras entidades que tenga contratadas, así como a terceros países u organizaciones internacionales.

h) Nombrar un delegado de protección de datos en los casos que fuera obligatorio y comunicar su identidad al Encargado.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Actualmente y a la fecha de suscripción del presente convenio de encomienda de gestión, 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. *Eficacia.*

De conformidad con el artículo 11 de la LRJSP, este convenio de encomienda de gestión surtirá efectos desde el momento de su firma y, para su plena eficacia, se publicará en el «Boletín Oficial del Estado».

Duodécima. *Comisión de Seguimiento.*

A instancia de cualquiera de las partes, podrá constituirse una Comisión Mixta con funciones de vigilancia y control, así como de resolución de cuestiones derivadas de los problemas de interpretación y cumplimiento del presente convenio de encomienda de gestión. Esta comisión tendrá carácter de órgano colegiado y en sus funciones se regirá por lo establecido en la LRJSP.

En caso de constituirse, estará formada por cuatro (4) representantes; dos (2) de los cuales representarán a la FNMT-RCM, E.P.E., M.P., y, otros dos (2) al Congreso de los Diputados, y se reunirá, al menos, una (1) vez al año.

Decimotercera. *Derecho aplicable y resolución de conflictos.*

El presente convenio lo suscribe el Congreso de los Diputados y la FNMT-RCM, E.P.E., M.P., para formalizar la encomienda de gestión objeto del mismo, de conformidad con el artículo 11 de la LRJSP, tiene naturaleza administrativa, y se regirá por lo expresamente pactado por las partes en este documento, por las normas citadas en el mismo y, en su defecto, por las normas de derecho administrativo que resulten de aplicación.

Sin perjuicio de la facultad de las partes de constituir la Comisión Mixta establecida en la cláusula duodécima, la realización de actividades previstas en este convenio y anexos, en cuanto al contenido y características de los mismos, se realizará con sujeción a la regulación contenida en la LPAC; en la Ley 6/2020, de 11 de noviembre; en 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.

Las partes se comprometen a resolver de mutuo acuerdo las incidencias que pudieran surgir en su interpretación y cumplimiento. Las cuestiones litigiosas que se suscitaran entre las partes durante el desarrollo y ejecución del convenio, se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la ley reguladora de la misma.

Y, en prueba de conformidad, ambas partes suscriben el presente convenio y todos sus anexos, en el lugar y fecha indicados en el encabezamiento. En Madrid, 30 de abril de 2026.–Por el Congreso de los Diputados, el Secretario General, Fernando Galindo Elola-Olaso.–Por la Fábrica Nacional de Moneda y Timbre, la Directora General, María Isabel Valldecabres Ortiz.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

ANEXO I

CAPÍTULO I

Servicios EIT

La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM, E.P.E., M.P.) presta servicios de certificación electrónica, que podemos dividir en los siguientes dos grupos.

Por un lado, servicios horizontales, que son aquellos servicios de carácter básico sobre los que se sustenta la labor de prestador de servicios de certificación. En ellos encontramos:

– Solicitud y descarga de certificados.
– Registro de usuarios.
– Gestión del ciclo de vida de certificados: emisión, revocación y archivo.
– Validación de certificados.
– Registro de eventos y archivo de evidencias.
– Atención a usuarios y soporte técnico.

Por otro, servicios específicos que se prestan a las Administraciones públicas en función de las necesidades de éstas. Son los servicios que se tarifican y que se encargan en la presente encomienda, según las unidades concretas que la entidad encargante necesite. Estos servicios incluyen:

– Certificado de empleado público.
– Certificado CERES Cloud ID (firma en la nube).
– Virtual Smart card para CERES Cloud ID.
– Certificados de componente: sellos electrónicos y certificados de autenticación de sitios web.
– Servicio de sellado de tiempo.

Los servicios contemplados en el presente anexo I se realizan de conformidad con lo establecido en la legislación aplicable a los mismos.

Se describen a continuación los servicios mencionados.

Servicios horizontales de certificación electrónica

La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM, E.P.E., M.P.), como prestador de servicios de certificación y de confianza, 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, E.P.E., M.P., 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, E.P.E., M.P., ofrecerá los siguientes servicios técnicos:

– Solicitud y descarga de certificados.
– Registro de usuarios.
– Gestión del ciclo de vida de certificados: emisión, revocación y archivo.
– Validación de certificados.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

– Registro de eventos y conservación de evidencias.
– Asistencia y soporte a usuarios.

Solicitud y descarga de certificados

La FNMT-RCM, E.P.E., M.P., habilitará los elementos necesarios para que el usuario final y solicitante del certificado pueda solicitar su certificado electrónico cualificado y descargarlo cuando su solicitud haya sido validada por un registrador autorizado.

La FNMT-RCM, E.P.E., M.P., establecerá los mecanismos necesarios durante el proceso de solicitud del certificado para garantizar que el usuario final, Titular o suscriptor del certificado, se encuentra en posesión de la clave privada asociada a la clave pública que será certificada.

A continuación, se enumeran los componentes involucrados en la solicitud y descarga de certificados:

Aplicación de solicitud de certificados

Aplicación que integra los elementos necesarios para activar, en el equipo del solicitante, la funcionalidad de generación y gestión segura del par de claves pública y privada, así como el envío de la clave pública a los repositorios de la FNMT-RCM, E.P.E., M.P., para su posterior certificación.

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, E.P.E., M.P.

Software de generación y gestión de las claves

Esta componente, desarrollado por FNMT-RCM, E.P.E., M.P., se integra en la aplicación de solicitud mencionada anteriormente. El software de generación de claves permitirá al usuario final generar de forma segura las claves criptográficas que le permitirán firmar e identificarse por medios telemáticos, así como proteger la seguridad de sus comunicaciones.

Adicionalmente, el software de generación de claves permitirá realizar la descarga e instalación segura del certificado al solicitante y Titular del certificado.

Aplicación de descarga de certificados

La aplicación de descarga de certificados integrará toda la funcionalidad necesaria para permitir que el solicitante y Titular del certificado pueda descargar e instalar de forma segura su certificado electrónico cuando su solicitud haya sido validada y aprobada por un registrador autorizado.

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, E.P.E., M.P.

Este registro podrá ser realizado por la propia FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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, E.P.E., M.P., 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, E.P.E., M.P., la persona que se encargue de la actividad de registro ha de

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

ser personal al servicio de la Administración pública. En estos casos la FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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 apartado 4 del artículo 7 de la Ley 6/2020, de 11 de noviembre. 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 la acreditación de identidad del interesado. Esta acreditación se puede realizar de forma remota, con video identificación, o presencial, requiriendo en este caso la presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. La acreditación de identidad con video identificación está excluida de la presente encomienda.

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, E.P.E., M.P., 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, E.P.E., M.P.

Si se trata de solicitudes relativas a certificados electrónicos a descargar en un servidor u otro componente, la FNMT-RCM, E.P.E., M.P., 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.

Gestión del ciclo de vida de certificados: emisión, revocación y archivo

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.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

La emisión de certificados por parte de la FNMT-RCM, E.P.E., M.P., solo puede realizarla ella misma, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos certificados.

La FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.

La FNMT-RCM, E.P.E., M.P., de forma previa la tramitación de una solicitud de emisión de certificado, comprobará:

a) Que el signatario es la persona identificada en el certificado.
b) Que el signatario tiene un identificador personal único.
c) Que el signatario dispone de la clave privada o acceso exclusivo a la misma en el caso de certificados de firma centralizada.

La FNMT-RCM, E.P.E., M.P., garantizará para cada 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.

Por su parte, la administración/organismo/entidad, que realiza la encomienda 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.P.E., M.P.

La administración/organismo/entidad que realiza la encomienda garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

a) A conservar su control exclusivo.
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.

La FNMT-RCM, E.P.E., M.P., una vez emitido el certificado, guardará registro del mismo 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.

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.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Revocación y suspensión de certificados electrónicos

La FNMT-RCM, E.P.E., M.P., 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 FNMT-RCM, E.P.E., M.P., 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 FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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 encomienda 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, E.P.E., M.P., suministrará a la administración/organismo/entidad que realiza la encomienda 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, E.P.E., M.P., 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 apartado 4 del artículo 9 de la Ley 6/2020, de 11 de noviembre, de Servicios electrónicos de confianza.

La administración/organismo/entidad y la FNMT-RCM, E.P.E., M.P., 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.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Registro y archivo de certificados y claves públicas

La FNMT-RCM, E.P.E., M.P., guardará registro de los certificados expedidos la información asociada, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de quince años.

Renovación de claves

La FNMT-RCM, E.P.E., M.P., 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.

CAPÍTULO II

Servicios avanzados

Certificados de componente

La FNMT-RCM, E.P.E., M.P., emite certificados de componente genérico, de servidor, por lo que se hereda la confianza que representa la FNMT-RCM, E.P.E., M.P., como Autoridad de Certificación instalada en los navegadores principales.

– Certificado de Sede Electrónica: certificado cualificado para la identificación de sedes electrónicas oficiales de la administración pública, organismos y entidades públicas vinculadas o dependientes.
– Certificado de autenticación de sitio web 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 de autenticación de sitio web 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 de autenticación de sitio web multidominio (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 electrónico para la Administración: 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.

Servicio de Sellado de Tiempo

La FNMT-RCM, E.P.E., M.P., es un Prestador de Servicios de Confianza, entre los que se incluye el Sellado de Tiempo o creación de sellos cualificados de tiempo electrónicos, conforme al Reglamentos elDAS, cuyo objeto es dar fe de la existencia de un conjunto de datos en un instante determinado en la línea de tiempo. Para ello utiliza como fuente de información temporal vinculada al Tiempo Universal Coordinado (UTC) la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada (ROA) en San Fernando, mediante el acuerdo alcanzado entre dicha Entidad y la FNMT-RCM, E.P.E., M.P., para la sincronización continua de sus sistemas.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

El ROA tiene como misión el mantenimiento de la unidad básica de tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala «Tiempo Universal Coordinado» (UTC-ROA), considerada a todos los efectos como la base de la hora legal en todo el territorio español (Real Decreto 1308/1992, de 23 de octubre de 1992).

El Sistema de Sincronismo con el Real Observatorio de la Armada (SS-ROA) instalado en el Centro de Proceso de Datos (CPD) de la FNMT-RCM, E.P.E., M.P., tiene como objetivo proporcionar una fuente de referencia temporal trazable a la escala de tiempo UTC (ROA), para la prestación del Servicio de Sellado de Tiempo de la FNMT-RCM, E.P.E., M.P.

Dicho sistema produce una serie de ficheros que contienen los datos de los seguimientos efectuados en un día y son utilizados por el ROA para elaborar los informes de diferencia de fase del patrón con la escala UTC (ROA).

La precisión declarada para la sincronización de la TSU con UTC es de 100 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. Por tanto, el Servicio de Sellado de Tiempo de la FNMT-RCM, E.P.E., M.P., no expedirá ningún sello de tiempo electrónico durante el periodo de tiempo en el que existiera un desfase mayor de 100 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del ROA.

La FNMT-RCM, E.P.E., M.P., suministrará a los Departamentos, organismos y entidades del sector público destinatarios de los servicios de la presente encomienda que así lo soliciten el acceso a este servicio de Sellado de Tiempo.

Tanto las peticiones de Sellado de Tiempo como las respuestas se gestionarán conforme a lo descrito en la recomendación RFC 3161.

Las respuestas de la Autoridad de Sellado de Tiempo, del tipo «application/timestamp reply», irán firmadas con un certificado con un tamaño de claves RSA de 3072 bits y algoritmo de firma SHA-256 y podrá validarse mediante cualquiera de los métodos de validación de los certificados que la FNMT-RCM, E.P.E., M.P., pone a disposición de los usuarios y terceras partes que confían en los certificados y que se describe en el apartado anterior.

La disponibilidad del Servicio es del 99.0 % y el tiempo medio de respuesta: 1 s o inferior en el 99 % de las peticiones.

CAPÍTULO III

Servicios Administración Pública (Ley 40/2015)

Servicio de Validación del Certificado de la AC Sector Público Lista de certificados revocados

Cuando un certificado es revocado, temporal o definitivamente, este es incluido en el Registro de certificados que conforma la lista de certificados revocados. Dicho registro comprende la información de todos los certificados expedidos por la FNMT-RCM, E.P.E., M.P., cuya vigencia se ha extinguido o suspendido, al menos hasta un año después de su fecha de caducidad.

La FNMT-RCM, E.P.E., M.P., publicará la lista de certificados revocados (CRLs) en un repositorio seguro que se actualiza de forma continuada con la información vigente. Las listas de revocación serán firmadas con la clave privada de firma de la FNMT-RCM, E.P.E., M.P.

Servicio de Validación

El servicio de validación de certificados, se prestará a través de los siguientes mecanismos:

– Servicio de consulta de CRLs mediante protocolo HTTP.
– Servicio de consulta de estado mediante protocolo OCSP.
– Aplicación de consulta de estado de certificado.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

La disponibilidad de múltiples servicios para la validación de certificados, proporciona compatibilidad total con las distintas necesidades de las aplicaciones en las que se utilizarán los certificados electrónicos.

La disponibilidad será del 99.0 % y el tiempo medio de respuesta será de 1 s o inferior para el 99 % de las peticiones.

Se podrán realizar consultas a este directorio en línea. Este servicio permite la disponibilidad continua y la integridad de la información almacenada en el directorio.

Servicio de consulta de CRLs mediante protocolo HTTP

Asimismo, la FNMT-RCM, E.P.E., M.P., publicará las CRLs en un repositorio público accesible mediante protocolo HTTP. De igual manera que en el caso anterior, este servicio podrá ser consultado en línea y mantendrá una versión vigente y actualizada de las CRLs.

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 Sector Público.

Este servicio se prestará desde la siguiente URL en el puerto estándar http 80:

– http://www.cert.fnmt.es/crlssp/CRLnnn.crl

Este punto de distribución de CRLs, irá insertado en todos los certificados de Entidad Final emitidos por la AC de Sector Público, 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, E.P.E., M.P., 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 consulta de estado OCSP

Además de publicar la lista de certificados revocados en los repositorios mencionados anteriormente, FNMT-RCM, E.P.E., M.P., pondrá a disposición de la entidad encargante un servicio de consulta del estado de validez de los certificados mediante protocolo Online Certificate Status Protocol (OCSP).

Aplicación de consulta de estado

Como complemento a los mecanismos de validación descritos anteriormente, FNMT-RCM, E.P.E., M.P., pone a disposición de los usuarios firmantes una aplicación para verificar el estado de sus certificados. Esta aplicación permite que un usuario final se autentique con su certificado y le muestre el estado de validez del mismo.

Registro de eventos y archivo de evidencias

Tipos de eventos registrados

La FNMT-RCM, E.P.E., M.P., 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.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

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, E.P.E., M.P., 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, E.P.E., M.P., mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a quince años.

En el caso del archivo histórico de los certificados, éstos permanecerán archivados durante al menos quince 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, E.P.E., M.P.

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, E.P.E., M.P.

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, E.P.E., M.P.

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, E.P.E., M.P., estime oportuno.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

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, E.P.E., M.P., garantiza la existencia de copias de seguridad de todos los registros auditados.

Certificado de empleado público

Los certificados electrónicos para el personal al servicio de las Administraciones públicas se emiten por la FNMT-RCM, E.P.E., M.P., por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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, E.P.E., M.P., como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 6/2020, de 11 de noviembre, 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) núm. 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.

FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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 de los certificados es el descrito en la declaración de prácticas de certificación correspondiente.

El compromiso de expedición del certificado son quince minutos, siendo el máximo asegurado de treinta minutos desde la solicitud en el modo *online*.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

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

Servicio de firma electrónica centralizada para empleados públicos (firma en la nube CERES Cloud ID).

La AC Sector Público 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 el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

El certificado de firma electrónica centralizada para empleados públicos es un certificado cualificado para la creación de firmas electrónicas cualificadas generadas en un dispositivo de creación de firma remoto, en un entorno seguro y confiable.

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 o sector público, 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 la seguridad (usuario+contraseña y segundo 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 Sector Público» subordinada de la «AC Raíz» de la FNMT-RCM, E.P.E., M.P.

Software de tarjeta virtual

La tarjeta virtual es un cliente-agente CSP (Cryptographic Service Provider) que permite utilizar los certificados electrónicos CERES Cloud ID directamente y de forma totalmente transparente desde el equipo del usuario como si estuvieran almacenados en un dispositivo cualificado de creación de firma basado en tarjeta inteligente. Esto permite la utilización directa de los certificados en las aplicaciones de escritorio y ofimáticas.

El software VSC consiste en un plugin de escritorio que proporciona el acceso a las claves de firma gestionadas por la plataforma de firma centralizada de la FNMT-RCM, E.P.E., M.P., Sus características principales son:

– Compatible con el almacén de certificados Microsoft Windows o PKCS#11 (Explorer, Chrome, Acrobat, Office, etc.).

– Permite integrar la firma remota usando las claves centralizadas conforme a la Regulación eIDAS.

– Permite usar los certificados CERES Cloud ID para autenticación TLS desde los navegadores web.

Se proveerán licencias de uso de Virtual Smart Card (VSC) para los equipos acordados en la duración del contrato.

Sello electrónico cualificado de las Administraciones públicas

Certificado cualificado de Sello electrónico para Administración Pública, órgano, organismo público o entidad de derecho público, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y con el Real

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, para la identificación y autenticación del ejercicio de la competencia y en la actuación administrativa/judicial automatizada de la unidad organizativa perteneciente a una Administración, organismo o entidad pública. 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) núm. 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.

Estos certificados cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las veinticuatro horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., 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 de sede electrónica de las Administraciones electrónicas

Certificados cualificados para la identificación de sedes electrónicas oficiales de la Administración pública, organismos y entidades públicas vinculadas o dependientes emitidos por la FNMT-RCM, E.P.E., M.P., bajo la denominación de certificados administración.

Se expiden de conformidad con los estándares europeos:

– ETSI EN 319 411-2 «Requirements for trust service providers issuing EU qualified certificates».
– ETSI EN 319 412-4 «Certificate profile for web site certificates».

Adicionalmente, cumplen con todos los requisitos establecidos por el CA/Browser Forum en sus especificaciones:

– «Baseline requirements for the issuance and management of publicly Trusted Certificates».
– «Guidelines for the issuance and management of extended validation certificates».

Estos certificados se expiden como cualificados conforme al Reglamento (UE) núm. 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

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

EN 319 411-1 «Policy and Security Requirements for Trust Services Providers issuing certificates-General Requirements.

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.

Estos certificados cuentan con servicio de validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las veinticuatro horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM, E.P.E., M.P., 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, E.P.E., M.P., de su alteración o modificación; todo ello, a través a través de las Oficinas de Registro habilitadas por las Administraciones, Organismos y Entidades públicas.

ANEXO II

Servicios EIT

Servicio	Importe/Unidad – Euros	Unidades/Año	Unidades totales	2026 – Euros	2027 – Euros	2028 – Euros	2029 – Euros	Importe total – Euros
Certificado empleado público con seudónimo								
– Bono 50 certificados.	476,00							
– Bono 200 certificados.	1.296,00							
– Bono 500 certificados.	2.637,00							
– Bono 1000 certificados.	5.168,00							
– Bono 5000 certificados.	23.490,00							
Certificado CERES Cloud ID (firma en la nube)								
– Bono 50 certificados.	500,00							
– Bono 200 certificados.	1.200,00							
– Bono 500 certificados.	2.800,00							
– Bono 1000 certificados.	5.500,00							
– Bono 5000 certificados.	25.000,00							
Virtual Smart Card para CERES Cloud ID								
– Pack 50 usuarios.	1.000,00							
– Pack 200 usuarios.	3.200,00							
– Pack 500 usuarios.	7.800,00							
– Pack 1000 usuarios.	15.500,00							
– Pack 5000 usuarios.	73.500,00							

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Servicio	Importe/Unidad – Euros	Unidades/Año	Unidades totales	2026 – Euros	2027 – Euros	2028 – Euros	2029 – Euros	Importe total – Euros
Certificados de componente								
– Sede electrónica.	510,00	1		510,00	510,00	510,00	510,00	2.040,00
– Autenticación sitio web estándar.	261,00							
– Autenticación sitio web wildcard.	534,00							
– Autenticación sitio web SAN (2 dominios).	309,00							
– Sellos electrónicos.	390,00	1		–	–	–	390,00	390,00
– Sello de entidad (1 año).	260,00							
– Sello de entidad (2 años).	330,00							
– Sello de entidad (3 años).	410,00							
Certificados de representación								
– Representante de persona jurídica.	14,00							
Registro de ciudadanos								
– Oficina de registro (3 registradores).	294,00							
– Registradores adicionales.	78,00							
Sellados de tiempo								
Pago por consumo (fijo 500 euros + variable)	500,00							
– 0 > n > 20.000	0,14							
– 20.000 > n > 40.000	0,13							
– 40.000 > n > 50.000	0,10							
– 50.000 > n > 60.000	0,09							
– 60.000 > n > 100.000	0,08							
– 100.000 > n > 175.000	0,05							
– 175.000 > n > 475.000	0,03							
– 475.000 > n > 1.000.000	0,03							
– 1.000.000 > n > 2.000.000	0,02							
– n > 2.000.000	0,02							
Tarifa plana por tramos								
– Hasta 10.000.	1.000,00							
– Hasta 25.000.	1.600,00							
– Hasta 30.000.	1.800,00							
– Hasta 60.000.	2.500,00							
– Hasta 100.000.	3.200,00							

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

Servicio	Importe/Unidad – Euros	Unidades/Año	Unidades totales	2026 – Euros	2027 – Euros	2028 – Euros	2029 – Euros	Importe total – Euros
Pack de servicios								
Población < 20.000 habitantes	488,00							
– Certificados de empleada/o público ilimitados. – 1 Sede electrónica S.P. – 1 Sello electrónico S.P. – 1 Certificado de componente o 1 oficina de registro (a elegir).								
Población < 20.000 + Sellado (10.000 sellados)	900,00							
Población > 20.000 habitantes	590,00							
– Certificados de empleada/o público ilimitados. – Sede electrónica S.P. – Sello electrónico S.P. – Certificado web estándard/sello de entidad/1 certificado wildcard/ 2 oficinas de registro ciudadanos (a elegir).								
Población > 20.000 + Sellado (10.000 sellados)	990,00							
Pack organismo sector público	1.500,00							
– Certificados de empleada/o público ilimitados. – Sede electrónica S.P. – Sello electrónico S.P. – 2 certificados de componente o 1 certificado wildcard (a elegir).								
Pack sector público + Sellado (10.000 sellados)	2.000,00	1	Certificados empleada/o público ilimitados. 4 Sedes electrónicas. 4 Sellos electrónicos. 8 certificados componente (SSL o sello).	2.000,00	2.000,00	2.000,00	2.000,00	8.000,00
Pack Diputaciones	1.500,00							
– Certificados de empleada/o público ilimitados. – Sede electrónica S.P. – Sello electrónico S.P. – 2 certificados de componente o 1 certificado wildcard (a elegir).								
Réplica LDAP CRLs	20.600,00							
Totales.				2.510,00	2.510,00	2.510,00	2.900,00	10.430,00

Compensación de gastos, de cuantía fija, para los servicios EIT en esta encomienda, en las anualidades 2026, 2027 y 2028 de la cantidad de dos mil quinientos diez euros

cve: BOE-A-2026-11243
Verificable en https://www.boe.es

(2.510,00 €) y en la anualidad 2029 la cantidad de dos mil novecientos euros (2.900,00 €), IVA excluido.

Servicio	Importe/Unidad – Euros	Unidades/Año	Unidades totales	2026 – Euros	2027 – Euros	2028 – Euros	2029 – Euros	Importe total – Euros
Certificados de componente								
– Sede electrónica.	510,00	1		510,00	510,00	510,00	510,00	2.040,00
– Sellos electrónicos.	390,00	1		–	–	–	390,00	390,00
Pack de servicios								
Pack sector público + Sellado (10.000 sellados)	2.000,00	1	Certificados empleada/o público ilimitados. 4 Sedes electrónicas. 4 Sellos electrónicos. 8 certificados componente (SSL o sello).	2.000,00	2.000,00	2.000,00	2.000,00	8.000,00
Totales.				2.510,00	2.510,00	2.510,00	2.900,00	10.430,00

Condiciones:

A todas las cantidades expuestas en este capítulo se les añadirá Impuesto de Valor Añadido según la legislación que sea de aplicación.

cve: BOE-A-2026-11243
Verificable en https://www.boe.es