III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA

20468 *Resolución de 7 de octubre de 2025, de la Dirección General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, por la que se publica el Convenio con el Defensor del Pueblo, para la extensión de los servicios públicos electrónicos.*

El Secretario General del Defensor del Pueblo y la Directora General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) han suscrito, con fecha de 19 de septiembre de 2025, un convenio para la extensión de los servicios públicos electrónicos.

De conformidad con lo dispuesto en el artículo 48 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 la Directora General de FNMT-RCM, en virtud de las competencias que tiene atribuidas de conformidad con el artículo 18 de los Estatutos de la Entidad, regulados por el Real Decreto 51/2023, de 31 de enero.

Madrid, 7 de octubre de 2025.–La Directora General de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, María Isabel Valldecabres Ortiz.

ANEXO

Convenio entre el Defensor del Pueblo y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, E.P.E., M.P., para la extensión de los servicios públicos electrónicos

REUNIDOS

De una parte, don José Manuel Sánchez Saudinós, Secretario General del Defensor del Pueblo, nombrado para este cargo por nombramiento interno por el Defensor del Pueblo de 2 de diciembre de 2021, en virtud de las competencias que le atribuyen los artículos 23 a 25 del Reglamento de Organización y Funcionamiento del Defensor del Pueblo, aprobado por las Mesas del Congreso de los Diputados y del Senado, en su reunión conjunta de 6 de abril de 1983, y conforme a la delegación de firma de 21 de marzo de 2024.

De otra, 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), con domicilio en la calle Jorge Juan núm. 106 de Madrid, en virtud de las competencias que le atribuye el artículo 18.3 de su Estatuto, aprobado por Real Decreto 51/2023, de 31 de enero (BOE núm. 27, de 1 de febrero), y de su nombramiento como Directora General mediante el Real Decreto 726/2021, de 3 de agosto (BOE núm. 185, de 4 de agosto).

Ambas partes intervienen en uso de las facultades que, de conformidad con la normativa vigente, les confieren los cargos que desempeñan y se reconocen mutuamente capacidad para la firma del presente convenio y, a tal efecto,

EXPONEN

Primero.

Que el Defensor del Pueblo, como alto comisionado de las Cortes Generales, es designado por éstas, de acuerdo con el artículo 54 de la Constitución, para la defensa de

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

los derechos comprendidos en el título I de la misma, a cuyo efecto podrá supervisar la actividad de la Administración, dando cuenta a las Cortes Generales.

Que corresponde al Secretario General el ejercicio de las funciones relativas al Servicio de Informática encargado del desarrollo de los sistemas de información necesarios para el funcionamiento de los servicios y de la implantación de la administración electrónica en la institución.

Segundo.

Que la FNMT-RCM, en correspondencia con los fines establecidos en su Estatuto, presta los servicios técnicos y administrativos necesarios para la identificación y autenticación de los intervinientes en las comunicaciones electrónicas con y entre las Administraciones Públicas, a través del uso de certificados de firma electrónica para funcionarios y demás empleados públicos, certificados de sede electrónica y certificados de sello electrónico para la actuación administrativa automatizada, en los que las Administraciones y organismos actúan, en sus registros y sedes electrónicas, a través de las oficinas de registro propias encargadas de acreditar y constatar los requisitos y condiciones especiales de utilización de estos servicios de confianza y certificación electrónica a prestar por la FNMT-RCM.

En las relaciones entre los ciudadanos e interesados y las administraciones públicas y demás órganos y organismos constitucionales y/o reguladores, se hace referencia a que los interesados podrán identificarse electrónicamente a través de, entre otros, sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la 'Lista de confianza de prestadores de servicios de certificación', que se elabore según establece el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y al amparo de 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 FNMT-RCM es uno de los prestadores de servicios de certificación incluidos en la «Lista de confianza» gestionada por el Ministerio para la Transformación Digital y de la Función Pública (Agencia Estatal de Administración Digital).

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

Tercero.

En relación con el presente convenio, ha de tenerse en cuenta la efectiva aplicación, desde el 1 de julio de 2016, del «REGLAMENTO (UE) n.º 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE», que es de directa aplicación en los Estados miembros.

Directamente vinculada con el Reglamento UE, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (que derogó la anterior Ley 59/2003, de 19 de diciembre, de firma electrónica), complementa los aspectos que el reglamento no ha armonizado o que ha dejado a los Estados su regulación y definición.

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 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPAC), y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tendrán plenos efectos jurídicos, entre ellos los sistemas proporcionados por la FNMT-RCM.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

Cuarto.

Como regulación especial de la FNMT-RCM, incorporada al artículo 4 de su Estatuto, se aprobó y mantiene su vigencia el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que faculta a la FNMT-RCM 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).

Que en relación con las funciones y competencias de la FNMT-RCM, el artículo 4.1. g) de su Estatuto regula la prestación de servicios de seguridad en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), así como 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.

Que el Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997 antes citado, regula el régimen de prestación de servicios de seguridad por la FNMT-RCM en la emisión y recepción de comunicaciones y escritos a través de medios y técnicas electrónicas, informáticas y telemáticas. Que su artículo 6, faculta a la FNMT-RCM 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.

Quinto.

La Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, 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.

En relación con la materia de este convenio, el Real Decreto 203/2021, de 30 de marzo, desarrolla la actividad de identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia, que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional y con seudónimo) y también regula la identificación y firma de los interesados y su representación.

Sexto.

Dado que es del interés general para las partes firmantes garantizar a los interesados que puedan relacionarse a través de medios electrónicos, y que la FNMT-RCM está en disposición de realizar las actividades técnicas y de seguridad relativas a la certificación y firma electrónica, según sus fines institucionales, las partes, en el ámbito de sus respectivas competencias, suscriben el presente convenio sobre la base de las siguientes

CLÁUSULAS

Primera. *Objeto del convenio.*

Constituye la finalidad de este convenio la creación del marco de actuación institucional entre las dos partes firmantes, que permita el impulso de servicios públicos

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

electrónicos de la FNMT-RCM, a través de la extensión al ámbito de competencias del Defensor del Pueblo de la Plataforma Pública de Certificación y de servicios electrónicos, informáticos y telemáticos desarrollada por la FNMT-RCM para su uso por las diferentes Administraciones.

En particular, la actividad de la FNMT-RCM comprenderá:

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

PACK Sector Público.
Certificados de empleada/o público ilimitados.

– 1 Sede electrónica S.P.
– 1 Sello electrónico S.P.
– 2 certificados de componente (2 sellos electrónicos S.P.).

* Estas cantidades son anuales.

2. Servicios complementarios:

La FNMT-RCM también prestará a petición del Defensor del Pueblo cualquiera, o la totalidad, de los servicios adicionales complementarios y/o suministros que, al efecto, se enumeran en los apartados de la siguiente condición y en el capítulo II, del mismo anexo I, de este convenio.

– 2 sellos electrónicos S.P. adicionales.

* Estas cantidades son anuales.

Segunda. *Ámbito de aplicación.*

A efectos del ámbito de aplicación, quedarán incluidos los servicios relativos a la identificación electrónica de las Administraciones Públicas y autenticación del ejercicio de su competencia y los servicios complementarios.

No podrán adherirse al presente convenio los organismos y entidades públicas dependientes, en su caso, del Defensor del Pueblo.

Tercera. *Compromisos de las partes.*

De acuerdo con el régimen de competencias y funciones propias de cada parte, corresponde a la FNMT-RCM, de acuerdo con lo dispuesto en el objeto de este convenio y en la normativa referida en el mismo, la puesta a disposición del Defensor del Pueblo, de la Plataforma Pública de Certificación desarrollada para la Administración Electrónica, para ofrecer seguridad en la utilización de instrumentos de identificación electrónica por parte de los ciudadanos. Estas Plataformas, junto con otras funcionalidades adicionales como el Sellado de Tiempo, permiten, a la FNMT-RCM, 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 Defensor del Pueblo la realización de las actuaciones administrativas y el desarrollo de sus competencias dirigidas a la implementación de las Plataformas en sus procedimientos.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

Para la adecuada consecución del objeto de este convenio, las partes han de desplegar una serie de actuaciones, que son:

1. La FNMT-RCM, realizará las siguientes actuaciones:

1.1 De carácter material, administrativo y técnico:

– Aportar la infraestructura técnica y organizativa adecuada para procurar la extensión e implementación de las Plataformas, con las funcionalidades previstas para el desarrollo de las relaciones administrativas de los ciudadanos, a través de sistemas EIT y de conformidad con lo contenido en los anexos y el estado de la técnica.

– Aportar los derechos de propiedad industrial e intelectual necesarios para tal implementación, garantizando su uso pacífico. La FNMT-RCM, excluye cualesquiera licencias o sublicencias, a terceras partes o a otras entidades para aplicaciones y sistemas de información propios o de terceros, distintas de las aportadas para ser utilizadas, en calidad de usuarios, directamente por la FNMT-RCM, en virtud de este convenio.

– Asistencia técnica, de conformidad con lo establecido en los anexos, con objeto de facilitar al Defensor del Pueblo la información necesaria para el buen funcionamiento de los sistemas.

– Actualización tecnológica de los sistemas, de acuerdo con el estado de la técnica y los Esquemas Nacionales de Interoperabilidad y Seguridad, sin perjuicio de la aprobación de los requisitos técnicos correspondientes por la Comisión de Estrategia Sobre Tecnologías de la Información y las Comunicaciones (CETIC) o, en su caso, por el órgano competente.

– Aportar la tecnología necesaria para que las obligaciones del Defensor del Pueblo, puedan ser realizadas; en particular las aplicaciones necesarias para la constitución de las Oficinas de Registro y Acreditación y la tramitación de las solicitudes de emisión de certificados electrónicos. Tales aplicaciones serán compatibles en función de los avances tecnológicos y el estado de la técnica.

– Emisión de informes, a petición del Defensor del Pueblo, acreditativos de la actividad de certificación realizada por la FNMT-RCM, en aplicación de este convenio.

– Tener disponible para consulta del Defensor del Pueblo 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. Tal DPC, estará disponible en la dirección electrónica (URL):

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

Esta DPC, podrá ser consultada por todos los interesados y podrá ser modificada por la FNMT-RCM, por razones legales o de procedimiento, estando siempre disponible la vigente y el histórico de versiones en las direcciones electrónicas especificadas en esta condición. Hay que tener en cuenta la parte general de la DPC y, para cada tipo de certificado o ámbito de actuación, las Políticas y Prácticas de Certificación Particulares aplicables específicamente, así como las Declaraciones Informativas PDSs, los Términos y Condiciones y los Perfiles de Certificados.

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

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

1.2 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 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 Defensor del Pueblo, llevará a cabo las siguientes actuaciones:

– Realizar las actividades de autoridad de registro consistentes en la identificación previa a la obtención del certificado electrónico y, en su caso, de comprobación y suficiencia de los atributos correspondientes, cargo y competencia de los firmantes/custodios, a través de la Oficina de Registro acreditada ante la FNMT-RCM, para las actividades que se relacionan seguidamente.
– Reconocer el carácter universal de los certificados de firma electrónica que expide la FNMT-RCM.
– Resolver los recursos y reclamaciones de su competencia.

3. Régimen de las Oficinas de Registro y Acreditación:

– General: Las aplicaciones informáticas necesarias para llevar a cabo las actividades de acreditación e identificación serán facilitadas por la FNMT-RCM al Defensor del Pueblo a través de los permisos correspondientes. Tales aplicaciones serán tecnológicamente compatibles en función de los avances tecnológicos y el estado de la técnica.

Las solicitudes de emisión y revocación y/o suspensión, en su caso, de certificados se ajustarán a los modelos establecidos por la FNMT-RCM y a los procedimientos recogidos en la Declaración de Prácticas de Certificación antes referenciada, así como a los procedimientos de registro de la FNMT–RCM.

Para los servicios de identificación y acreditación de los empleados del Defensor del Pueblo: Las Oficinas de Registro y Acreditación de los empleados del Defensor del Pueblo dependerán orgánica y funcionalmente de ella (sin perjuicio de las funciones de comprobación, coordinación y control de la FNMT-RCM) y determinarán la identidad y competencia del propio Defensor del Pueblo 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: http://www.cert.fnmt.es/dpc/ape/dpc.pdf 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 Defensor del Pueblo dispondrá de las Oficinas de Registro y Acreditación que considere necesarias para la acreditación de este tipo de certificados y deberán contar con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM y realizar las solicitudes de emisión de los certificados. En 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 y de conformidad con la DPC General y la específica Política y Prácticas de Certificación particulares correspondientes a estos certificados.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

Las acreditaciones realizadas por las personas, entidades y corporaciones a que se refiere el apartado nueve del artículo 81 de la Ley 66/1997, de 30 de diciembre, citada, y por los diferentes órganos y organismos públicos de la Red de Oficinas de Registro y acreditación, surtirán plenos efectos y serán válidas para su aceptación por cualquier administración pública que admita los certificados emitidos por la FNMT-RCM.

Cuarta. *Reembolso de gastos.*

1. Reembolso de gastos por colaboración administrativa en materia de certificación electrónica.

La FNMT-RCM percibirá anualmente, por los servicios recogidos en el capítulo II (Servicios Avanzados) y en el capítulo III (Servicios AP) del anexo I, prestados al Defensor del Pueblo, la cantidad total de 2.280,00 euros (dos mil doscientos ochenta euros), IVA excluido.

En caso de que el período inicial de duración del convenio sea inferior a un año, la cantidad anterior se prorrateará, reduciéndose proporcionalmente a su duración inicial.

Si hubiera petición expresa, por parte del Defensor del Pueblo, de extensión de otras funcionalidades de entre las recogidas en los capítulos II y III, del anexo II, la cantidad anterior quedaría incrementada por el importe correspondiente que se dedujera de la aplicación de las tablas contenidas en dicho anexo II, de Memoria Económica, del presente convenio.

2. Reembolso en años sucesivos.

Para sucesivos años, se aplicará el mismo criterio en función de las compensaciones a percibir, servicios solicitados y prórrogas del convenio.

3. Facturación.

El pago por los servicios prestados por la FNMT-RCM, que incluirá, en su caso, los servicios adicionales solicitados, se efectuará a la finalización de la prestación del servicio en cada anualidad. Regla del Servicio Hecho.

El abono de las facturas se realizará mediante transferencia bancaria a la cuenta de la FNMT-RCM en un plazo no superior a treinta días a contar desde la recepción de la factura que habrá sido emitida en el último trimestre del año:

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

Para proceder al pago de la factura la FNMT habrá remitido previamente Certificado de Titularidad Bancaria de la cuenta en la que deba abonarse la factura.

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

Denominación Defensor del Pueblo Ley Orgánica 3/81.
Calle: Eduardo Dato, 31.
Población: Madrid.
Provincia: Madrid.
NIF/CIF: S2804005C.
Departamento o persona de contacto: Servicio de Régimen Económico.

Las facturas serán emitidas en formato electrónico y remitidas a través del Punto General de entrada de facturas electrónicas de la Administración General del Estado.

(FACE) con los siguientes datos DIR3:

I00000007 Oficina Contable
I00000007 Órgano Gestor
I00000007 Unidad Tramitadora

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

Quinta. *Comisión de seguimiento, vigilancia y control.*

A instancias de cualquiera de las partes, podrá constituirse una Comisión de Seguimiento, Vigilancia y Control de la ejecución del presente convenio y de los compromisos adquiridos por los firmantes, así como de resolución de cuestiones derivadas de los problemas de interpretación y cumplimiento. Esta Comisión tendrá carácter de órgano colegiado y su funcionamiento se regirá por lo establecido en la Ley 40/2015, de 1 de octubre.

Sexta. *Vigencia del convenio.*

Este convenio se perfecciona por la prestación del consentimiento de las partes y resultará eficaz una vez inscrito en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal y publicado en el «Boletín Oficial del Estado», conforme a lo establecido en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El convenio tendrá una duración de cuatro años. Los firmantes del mismo podrán acordar unánimemente su prórroga por un periodo de otros cuatro años adicionales o su extinción conforme a lo dispuesto en el artículo 49.h) 2.º de la Ley 40/2015, de 1 de octubre.

Para materializar la prórroga, antes del vencimiento inicial del convenio, ambas partes suscribirán una adenda en la que se establecerán sus condiciones.

Séptima. *Revisión.*

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

La modificación del convenio deberá realizarse por acuerdo unánime de las partes y se formalizará mediante adenda.

Octava. *Responsabilidad.*

El Defensor del Pueblo y la FNMT-RCM, a los efectos previstos en el objeto de este convenio, responderán cada una en el ámbito de sus respectivas funciones y competencias, en relación con los daños y perjuicios que causara el funcionamiento del sistema de acuerdo con las reglas generales del ordenamiento jurídico que resultarán de aplicación y de conformidad con las obligaciones asumidas a través del presente convenio.

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

Novena. *Extinción y resolución.*

El convenio se extingue por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución.

Son causas de resolución del convenio:

– El transcurso del plazo de vigencia del convenio sin haberse acordado la prórroga del mismo.

– El acuerdo unánime de resolución de las Partes.

– El incumplimiento de las obligaciones y compromisos asumidos por alguna de las partes. En este caso, cualquiera de las partes podrá notificar a la parte incumplidora un requerimiento para que cumpla en un determinado plazo con las obligaciones o compromisos que se consideran incumplidos. Este requerimiento será comunicado al Presidente de la Comisión de seguimiento, vigilancia y control de la ejecución del

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

convenio, en el caso de que esta se haya constituido, y a las demás partes firmantes. Si trascurrido el plazo indicado en el requerimiento persistiera el incumplimiento, la parte que lo dirigió notificará a las partes firmantes la concurrencia de la causa de resolución y se entenderá resuelto el convenio. La resolución del convenio por esta causa podrá conllevar la indemnización de los perjuicios causados a la parte que los hubiera sufrido, de conformidad con las reglas del ordenamiento jurídico de aplicación.

– Por decisión judicial declaratoria de la nulidad del convenio.

– Por cualquier otra causa distinta de las anteriores prevista en el convenio o en otras leyes.

Décima. *Protección de datos de carácter personal.*

Régimen

El régimen de protección de datos de carácter personal derivado de este convenio y de la actuación conjunta de las partes, será el previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos-RGPD); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y en el Real Decreto 1720/2007, de 21 de diciembre, en lo que no se oponga a las normas antes citadas.

La FNMT-RCM ha creado un Registro de Actividades de Tratamiento y nombrado a un Delegado de Protección de Datos, con el fin de adaptarse al RGPD, que pueden consultarse en http://www.fnmt.es/rgpd

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

El Defensor del Pueblo 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.defensordelpueblo.es/privacidad/

– Delegado de Protección de Datos del Defensor del Pueblo.
– Email: dpo@defensordelpueblo.es
– Dirección: Calle Zurbano, 42, CP: 28010 Madrid.

Comunicación de datos

La comunicación de datos de carácter personal que el Defensor del Pueblo realice a la FNMT-RCM sobre los datos de los empleados públicos de aquélla para la emisión de certificados de firma electrónica en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (y, en su caso, en el del 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 de aplicación (RGPD, artículo 13 y LOPDGDD, artículo 11), según consta en el Registro de Actividades de Tratamiento antes señalado (Tratamiento n.º 13).

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

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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

1) No tendrá carácter de comunicación de datos el acceso que el Defensor del Pueblo, en calidad de Oficina de Registro y Acreditación de la FNMT-RCM, realice sobre los datos de carácter personal que la FNMT-RCM mantiene, como Responsable del tratamiento, sobre sus usuarios, personas físicas, con la finalidad de solicitar los servicios EIT en el ámbito del 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, descrito en el enlace anterior.

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

3) Las actuaciones concretas que sobre el Tratamiento n.º 13 del RAT de la FNMT-RCM que el Defensor del Pueblo realizará sobre los datos serán los siguientes:

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

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

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

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

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

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

Todo el personal al que el Encargado proporcione acceso a los datos personales deberá ser informado, de forma expresa, a respetar la confidencialidad y a cumplir las

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

d) Llevar por escrito y estar disponible, un Registro Actividades de Tratamiento efectuados por cuenta del Responsable, que contenga (en su caso): las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

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

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

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

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

f) No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del Encargado.

El Encargado podrá comunicar los datos a otros encargados del tratamiento del mismo Responsable, previo consentimiento y de acuerdo con las instrucciones del Responsable, indicando los tratamientos que se pretenden subcontratar e identificando, de forma clara e inequívoca, la empresa subcontratista y sus datos de contacto.

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

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

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

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

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

1. Acceso, rectificación, supresión y oposición.
2. Limitación del tratamiento.
3. Portabilidad de datos.
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

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

l) Devolver al Responsable los datos de carácter personal que hayan sido objeto de tratamiento. En todo caso, el encargado podrá conservar debidamente bloqueados

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

aquellos datos que sean necesarios, en tanto pudieran derivarse responsabilidades de su relación con el Responsable del tratamiento.

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

a) Facilitar al Encargado el acceso a los datos que forman parte de sus ficheros o entregárselos del modo que resulte oportuno para la correcta prestación del servicio.
b) Informar conforme a la normativa a los interesados cuyos datos sean objeto de tratamiento y haber obtenido de los mismos lícitamente su consentimiento expreso o contar con motivos legítimos y acreditables para el mismo.
c) Tener establecida la base legal que legitima el tratamiento.
d) Disponer de mecanismos sencillos para que los interesados puedan ejercitar sus derechos.
e) Contar con análisis de riesgos, con un registro de los tratamientos y evaluaciones de impacto si fuera necesario por la naturaleza de los datos tratados.
f) Tener habilitadas las medidas de seguridad adecuadas para salvaguardar los datos en la transmisión de los datos al Encargado.
g) Nombrar un delegado de protección de datos en los casos que fuera obligatorio y comunicar su identidad al Encargado. Actualmente y a la fecha de suscripción del presente contrato los datos del Delegado de Protección de Datos nombrado por la FNMT-RCM son los siguientes:

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

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

Undécima. *Derecho aplicable y resolución de conflictos.*

El presente convenio tiene naturaleza administrativa. Se regulará por lo establecido en el mismo, quedando excluido del ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, conforme a lo dispuesto en su artículo 6.

Sin perjuicio de la facultad de las partes de constituir la Comisión de Seguimiento, Vigilancia y Control establecida en la cláusula cuarta, la realización de actividades previstas en este convenio, en cuanto al contenido y características de estas, se realizará con sujeción a sus cláusulas y a la regulación contenida en el mismo.

Las partes se comprometen a resolver de mutuo acuerdo las incidencias que pudieran surgir en su interpretación y cumplimiento. Las controversias sobre la interpretación y ejecución del presente convenio serán resueltas en el seno de la comisión de seguimiento y, en el caso de que no fuera posible, el orden jurisdiccional contencioso administrativo será el competente para resolver las cuestiones litigiosas que pudieran suscitarse entre las partes de conformidad con lo dispuesto en los artículos 1 y 2 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso administrativa.

Y, en prueba de conformidad, las partes firman el presente Convenio a 19 de septiembre de 2025.–El Defensor del Pueblo, José Manuel Sánchez Saudinós.–Por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, María Isabel Valldecabres Ortiz.

cve: BOE-A-2025-20468
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 el presente convenio, 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-2025-20468
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. 1.

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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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 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 del presente convenio.
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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

La emisión de certificados por parte de la FNMT-RCM, E.P.E., M.P., sólo 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 el convenio 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 el convenio 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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 convenio 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 el convenio 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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 15 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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 octubre 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 del presente convenio 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: 1s 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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 1s 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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 15 años.

En el caso del archivo histórico de los certificados, éstos permanecerán archivados durante al menos 15 años.

Datos relevantes que serán registrados:

Serán registrados los siguientes eventos relevantes:

a) La emisión y revocación y demás eventos relevantes relacionados con los certificados.

b) Todas las operaciones referentes a la firma de los certificados por la FNMT-RCM, 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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.

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) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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 15 minutos, siendo el máximo asegurado de 30 minutos desde la solicitud en el modo online.

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.

Los Certificados de firma electrónica centralizada para empleado público expedidos por la FNMT-RCM, E.P.E., M.P. tendrán validez durante un periodo máximo de tres (3) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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 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) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

La duración de este tipo de certificados es de 3 años.

Estos certificados cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM, 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.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

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) N.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, de conformidad con los estándares europeos ETSI 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.

La duración de los mismos se establece en 1 año.

Estos certificados cuentan con servicio de validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

FNMT-RCM, 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

Memoria Económica

Servicios de certificación electrónica

Se establece la siguiente compensación anual para la prestación de las siguientes cantidades anuales de servicios de certificación electrónica:

– Certificados de componente (Sellos electrónicos): 780.00 euros.

- Importe/unidad: 390,00 euros.
- Unidades por año: 2.
- Unidades totales: 8.
- Compensación total (años 2026 a 2029): 3.120,00 euros.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es

– Pack de servicios (pack organismo sector público): 1.500,00 euros.

- Importe/unidad: 1.500,00 euros.
- Unidades por año: 1.
- Unidades totales: 4.
- Compensación total (años 2026 a 2029): 6.000,00 euros.

El pack de organismo sector público comprende: Certificados de empleada/o públicos ilimitados, 4 sedes electrónicas, 4 sellos electrónicos, 8 certificados de componente.

– Compensación total anual: 2.280, 00 euros.
– Compensación total (años 2026 a 2029): 9.120,00 euros.

cve: BOE-A-2025-20468
Verificable en https://www.boe.es