TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE SELLOS ELECTRÓNICO POR LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, E.P.E., M.P. (FNMT-RCM).

El *Solicitante* manifiesta que utilizará el *Certificado* de conformidad con las condiciones adjuntas y atendiendo al contenido de la Declaración General de Prácticas de Servicios de Confianza y de Certificación Electrónica y de las Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónicos de la FNMT-RCM, declarando expresamente que las acepta en toda su extensión y que su capacidad no se encuentra limitada para realizar esta solicitud y contratar con esta Entidad.

Estas condiciones son un extracto de las *Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónicos de* la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, E.P.E., M.P. (FNMT-RCM), con las normas básicas para la expedición de estos *Certificados*. Se pone a disposición del *Solicitante* la siguiente información básica, quedando satisfecho el deber de información con la *Declaración General de Prácticas de Servicios de Confianza y de Certificación Electrónica* (DGPC) y con las Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónico, puestas a disposición en formato digital en los enlaces anteriores.

Tipo de certificado y límites de uso

La Autoridad de Certificación expide los *Certificados de Sello Electrónico* como sistema de identificación para la actuación administrativa automatizada y para la actuación judicial automatizada.

Estos *Certificados de Sello Electrónico:*

- 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.
- Son expedidos a organismos y que forman parte de la Comunidad Electrónica, tal y como se define en la DGPC de la FNMT-RCM, y con objeto de garantizar el origen y la integridad de los contenidos mediante la creación del Sello electrónico.
- Son cualificados en cumplimiento con los requisitos del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por el que se deroga la directiva 1999/93/CE.

Estas Condiciones de Utilización no alteran o modifican la naturaleza, régimen jurídico y competencias de la Administración, Organismo o Entidad pública y del personal donde desarrolla su función pública o actividad, por lo que FNMT-RCM no será responsable de las actuaciones que se realicen con los certificados emitidos, por cuestiones que no tengan su origen, únicamente, en la organización y funcionamiento de la FNMT-RCM en las condiciones expuestas en las Políticas y Prácticas de Certificación antes citadas.

Constituyen límites de uso de los Certificados de Sello Electrónico la creación de sellos electrónicos de Administración Pública, organismo o entidad de derecho público, 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.

Validez de los Certificados

Los Certificados de Sello Electrónico, expedidos por la FNMT-RCM, tendrán la validez establecida en sus Políticas y Prácticas de Certificación particulares, contado 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*.

Los *Certificados de Sello Electrónico* no podrán ser utilizados cuando expire su periodo de validez, cuando sea solicitada su revocación o se cumpla alguna de las otras causas de extinción de su vigencia, establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y en las *Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónicos.*

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el Protocolo de Verificación de Certificados en Línea (OCSP, por sus siglas en inglés), disponible en la ubicación especificada en el propio certificado.

Renovación de los Certificados

La FNMT-RCM no contempla la posibilidad de renovar los Certificados de Sello Electrónico. Una vez caducado el Certificado, se deberá solicitar uno nuevo para poder seguir utilizando los servicios del Proveedor de Servicios de Confianza.

Revocación de los Certificados

La solicitud de revocación de los Certificados de Sellos Electrónicos podrá efectuarse durante el período de validez que consta en los Certificados.

La revocación de un *Certificado de Sello Electrónico* podrá ser solicitada por:

- La Autoridad de Certificación y la Autoridad de Registro.
- El suscriptor a través de su representante o persona autorizada, en la Oficina de Registro habilitada a tal efecto.
- En su caso, el Firmante, a través del teléfono habilitado para tal fin (previa identificación de (Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7, o bien a través de dicha Oficina de Registro.

También será causa de revocación de un Certificados de Sellos Electrónicos la solicitud de un nuevo Certificado del mismo tipo y mismos datos emitido por la FNMT-RCM.

Finalmente, serán causas de revocación las establecidas en las Políticas de Certificación.

La revocación de un Certificado anulará su validez antes de la fecha de caducidad que consta en el mismo.

Obligaciones de la Oficina de Registro

De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la DGPC, las *Oficinas de Registro* y el Responsable de Operaciones de Registro, en el caso de los Certificado de Sello Electrónico, tienen la obligación de:

- Comprobar fehacientemente los datos referidos a la identidad y a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del Personal al servicio de la Administración Pública como firmante del Certificado, con la Administración, organismo o entidad a la que presta sus servicios (Suscriptor del Certificado).
- El Prestador de Servicios de Confianza, a través del Responsable de Operaciones de Registro velará por el cumplimiento de los procedimientos aprobados por FNMT-RCM en materia de identificación de los Solicitantes de los Certificados e informará a los usuarios de los Certificados sobre su adecuado uso, de conformidad con las condiciones de uso, las Políticas y Prácticas de Certificación y la normativa aplicable.
- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una entidad diferente a la que representa, o sobre la que no se tiene potestad o competencia para actuar como Oficina de Registro, sin perjuicio de la creación de Oficinas de Registro centralizadas o de convenios entre administraciones para efectuar registros.
- No realizar registros o tramitar solicitudes de Certificados emitidos bajo estas políticas y cuyo Solicitante no haya sido autorizado por el Responsable de Operaciones de Registro.
- Solicitar la revocación del Certificado de Firma Electrónica desde que se tenga conocimiento cierto de cualquiera de los hechos determinantes especificados en el apartado 4.9.1 de las Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónicos.

Obligaciones del Suscriptor y del firmante o solicitante

De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Personal al servicio de la Administración Pública*, como *Firmante* del *Certificado,* y/o en su caso el suscriptor de los mismos, tienen la obligación de:

- No utilizar el Certificado cuando alguno de los datos incluidos sea inexacto o incorrecto; o no refleje su relación con el órgano en el que presente el servicio o existan razones de seguridad que así lo aconsejen
- Realizar un uso adecuado del Certificado en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o empleo como Personal al servicio de la Administración Pública.
- Comunicar al Responsable de Operaciones de Registro, cualquiera de los hechos determinantes especificados en el apartado 4.9.1 de esta DPPP, con el fin de iniciar los trámites de revocación su Certificado.
- No usar el Certificado fuera de los límites especificados en su Política y Prácticas de Certificación particulares.
- No usar el Certificado en caso de que el Prestador de Servicios de Confianza haya cesado su actividad como Entidad emisora de Certificados que expidió el certificado en cuestión, especialmente en los casos en los que los Datos de Creación de Firma del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los Certificados y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- Actuar con diligencia respecto de la custodia y conservación de los Datos de Creación de Firma o cualquier otra información sensible como Claves, códigos de activación del Certificado, palabras de acceso, números de identificación personal, etc., así como de los soportes de los Certificados, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los Certificados previstas en las condiciones de uso y en la Declaración de Prácticas de Certificación y en particular, las limitaciones de uso de los Certificados.
- Conocer y cumplir las modificaciones que se produzcan en la Declaración de Prácticas de Certificación.
- Solicitar la revocación del correspondiente Certificado, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM, las circunstancias para la revocación o sospecha de pérdida de la Confidencialidad, la divulgación, modificación o uso no autorizado de los Datos de Creación de Firma.
- Revisar la información contenida en el Certificado, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los Certificados, la Firma electrónica reconocida del Prestador de Servicios de Confianza emisor del Certificado.
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del Certificado, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.
- Devolver o destruir el Certificado cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el Certificado caduque, o sea revocado.
- No solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.

Será responsabilidad del Firmante informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el Certificado, para su revocación y nueva expedición.

Obligaciones de verificación del estado de los certificados de las terceras partes

El resto de la Comunidad Electrónica, Entidades usuarias y los terceros regularán sus relaciones con la FNMT-RCM a través de la DGPC y, en su caso, a través de las Políticas y Prácticas de Certificación; todo ello sin perjuicio de lo dispuesto en la normativa sobre Firma Electrónica y demás normativa que resulte de aplicación.

Los miembros de la Comunidad Electrónica, Entidades usuarias y los terceros que confían en los Certificados y en las Firmas electrónicas generadas con los mismos, deberán conocer las Políticas y Prácticas de Certificación y cumplir las siguientes obligaciones, exonerando de cualquier responsabilidad al Prestador de Servicios de Confianza en caso de que alguna no sea cumplida:

- Verificar con carácter previo a confiar en los Certificados de Sello avanzados del Prestador de Servicios de Confianza que expidió el Certificado.

- Verificar que el Certificado del firmante continúa vigente.
- Verificar el estado de los Certificados en la cadena de certificación, mediante consulta al Servicio de información y consulta sobre el estado de validez de los certificados de la FNMT-RCM.
- Comprobar las limitaciones de uso contenidas en el Certificado que se verifica.
- Conocer las condiciones de utilización del Certificado conforme a la Declaración General de Prácticas de Servicios de Confianza y Certificación Electrónica.
- Notificar a la FNMT-RCM o a cualquier Oficina de Registro, cualquier anomalía o información relativa al Certificado y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

Limitaciones de responsabilidad

La FNMT-RCM únicamente responde de la correcta identificación personal del Solicitante y futuro Titular, y de incorporar esos datos a un Certificado. Para la aplicación de garantías, obligaciones y responsabilidades, es necesario que el hecho se haya producido en el ámbito de la Comunidad Electrónica.

La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como Prestador de Servicios de Confianza, y conforme a lo dispuesto en estas Políticas de Certificación o en la Ley. En ningún otro caso será responsable de las acciones o de las pérdidas en las que incurran los Titulares, Suscriptores, Entidades usuarias, o terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados procedimientos de expedición y/o de gestión de los Certificados.

FNMT-RCM no responderá en caso de fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT-RCM podrá establecer cláusulas de limitación de responsabilidad. En todo caso, la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a terceros perjudicados, y/o miembros de la Comunidad electrónica en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€) euros.

La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los Certificados haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en las Políticas y Prácticas de Certificación y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente. No obstante, la FNMT-RCM pondrá las medidas de protección adecuadas para la protección de sus sistemas frente a Software malicioso (Malware) y las mantendrá diligentemente actualizadas para colaborar con los usuarios en evitar los daños que este tipo de software puede causar.

La FNMT-RCM no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en la Declaración de Prácticas de Certificación y en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

En caso de terminación de la actividad del Prestador de Servicios de Certificación, la FNMT – RCM se regirá por lo dispuesto en la normativa vigente sobre firma electrónica. En todo caso, informará debidamente y con antelación suficiente a los titulares de los certificados, así como a los usuarios de los servicios afectados y transferirá, con el consentimiento expreso de los titulares, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Certificación que los asuma. De no ser posible esta transferencia la vigencia de los certificados quedará extinguida

La FNMT – RCM registra y mantiene archivados aquellos eventos significativos necesarios para verificar la actividad de esta Autoridad de Certificación durante un periodo nunca inferior a quince (15) años, conforme a la legislación aplicable.

En cualquier caso, las limitaciones aquí recogidas no tienen carácter exhaustivo por lo que se estará también a lo dispuesto en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y en las Políticas y Prácticas de Certificación Particulares de los Certificados de Sello Electrónicos de la FNMT-RCM.

Política de devolución

En un contexto de buenas prácticas empresariales la FNMT - RCM ha adoptado una política de devolución del certificado emitido que permite la solicitud de reembolso dentro del periodo de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado.

Ley aplicable, quejas y resolución de disputas

La provisión de servicios de confianza de la FNMT – RCM se regirá por lo dispuesto por las Leyes del Reino de España. Con carácter general, los miembros de la Comunidad Electrónica y los Usuarios de los servicios de confianza de la FNMT-RCM aceptan que todo litigio, discrepancia, cuestión o reclamación resultante de la ejecución o interpretación de las Políticas y/o Declaraciones de Prácticas de Servicios de Confianza y de Certificación electrónica o relacionada con ellas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos, condiciones generales y/o encomiendas o convenios, en los términos previstos en el Estatuto de la entidad, aprobado por Real Decreto 51/2023, de 31 de enero (BOE nº 27 de 1 de febrero de 2023).

En caso de que los contratos, condiciones generales y/o encomiendas o convenios, no especificasen sistemas de resolución de conflictos, todas las partes se someten a la jurisdicción exclusiva de los tribunales del Estado español en la ciudad de Madrid. Asimismo, podrán pactarse, previa aprobación de los órganos competentes de la FNMT-RCM, procedimientos de mediación o arbitraje, de acuerdo con lo establecido en la legislación aplicable.

Asimismo, podrán pactarse, previa aprobación de los órganos competentes de la FNMT-RCM, procedimientos de mediación o arbitraje, de acuerdo con lo establecido en la legislación aplicable.
De acuerdo con lo dispuesto en el apartado 9.13 de la Declaración General de Prácticas de Servicios de Confianza y de Certificación

electrónica , la FNMT-RCM, atenderá cualquier solicitud, queja o reclamación por parte de sus clientes o terceros que confían en sus servicios de confianza, de conformidad con los protocolos aprobados por dicha Entidad mediante los procedimientos internos "Protocolo para la gestión de acciones correctivas, preventivas y de mejora", "Protocolo para la gestión de sugerencias, quejas y reclamaciones" y "Protocolo para la gestión de incidencias".

Cualificación y auditoría

Desde la entrada en vigor del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social y sus modificaciones, la FNMT-RCM ha logrado impulsar significativamente la extensión de sus servicios, especialmente en el ámbito de la Certificación Electrónica, consolidándose como un referente destacado en la Prestación de Servicios de Confianza.

La FNMT – RCM, como Prestador de Servicios de Confianza, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplican especialmente a estos tipos de certificados de sello los estándares europeos:

- ETSI EN 319 411-1 "Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements"
- ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates"
- ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons

Esta auditoría se lleva a cabo con la periodicidad requerida y por un Organismo de Evaluación de la Conformidad acreditado para tal fin.

Los Certificados de Sello Electrónico se expiden como cualificados conforme al Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza de España, a través del enlace https://sedediatid.mineco.gob.es/Prestadores

Información de contacto del Prestador de Servicios de Confianza

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda C/ Jorge Juan, 106

28009 Madrid

https://www.sede.fnmt.gob.es/

Contacto: ceres@fnmt.es

La FNMT-RCM pone a disposición de los Suscriptores, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de Certificados, en cuanto a un supuesto compromiso de Clave Privada, uso indebido de los Certificados u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

PROTECCIÓN DE DATOS

Le ofrecemos información básica sobre los datos de carácter personal recogida. Esta información se realiza en dos capas sobre la base de la regulación europea (arts. 13 y 14 del REGLAMENTO (UE) 2016/679 - Reglamento General de Protección de Datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Puede seguir los enlaces para obtener información más detallada.

RESPONSABLE: FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, E.P.E., M.P. (FNMT-RCM)

FINALIDAD: gestión de la prestación de servicios de confianza y demás servicios de la Administración Electrónica y Sociedad de la Información, relacionados y previstos en los fines de la Entidad y en la normativa vigente. Gestionar la prestación de los anteriores servicios en todas las fases de su desarrollo y ejecución. Gestión de calidad, consultas y sondeos de opinión relacionados con los servicios de confianza.

LEGITIMACIÓN: ejecución de un contrato para la prestación de un servicio del que los interesados son parte. Cumplimiento de una obligación legal aplicable al responsable del tratamiento. Art. 6.1.c) RGPD y Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

COMUNICACIONES DE DATOS: Administraciones públicas, organismos y entidades vinculadas o dependientes, en el ámbito del artículo 81 de la ley 66/1997, de 30 de diciembre y el resto de supuestos contemplados en normas europeas y nacionales con rango de Ley. Se producirán comunicaciones de datos al incluir el número de serie del Certificado en la lista de Certificados revocados. Además, el uso del Certificado posibilita que los terceros puedan acceder a datos que nos ha proporcionado (nombre, apellidos y DNI). Comunicaciones a las Fuerzas y Cuerpos de Seguridad del Estado y órganos judiciales. No se realizan transferencias internacionales fuera de la UE.

DERECHOS: puede acceder, rectificar, suprimir los datos y ejercitar el resto de derechos, según se informa en https://www.fnmt.es/politica-privacidad

PROCEDENCIA: consentimiento inequívoco del interesado. De empresas y organizaciones donde prestan servicios los interesados.

MEDIDAS DE SEGURIDAD: Esquema Nacional de Seguridad. Más información en enlace inferior.

CATEGORÍA DE DATOS: Datos identificativos: NIF/DNI, Pasaporte (contenido completo), nombre y apellidos, dirección, teléfono, edad, fecha de nacimiento, correo electrónico, cargo, denominación o razón social, IP, NICC (Número de Identificación Central Consular). Datos de certificado electrónico: clave pública de autenticidad, clave privada para firma en la nube, número de serie del certificado, código de solicitud del certificado. Datos de circunstancias sociales/legales: atributos relativos a la capacidad y poder de representación. Datos de información comercial: dirección electrónica (URL).

Puede consultar información adicional y detallada sobre este tratamiento en: https://www.fnmt.es/politica-privacidad (TRATAMIENTO Nº 13)