TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE FIRMA ELECTRÓNICA Y SELLO ELECTRÓNICO PARA EL SECTOR PÚBLICO EMITIDOS POR LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (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 de certificados de firma electrónica y Sello Electrónico del Sector Público (https://www.sede.fnmt.gob.es/dpcs/acsp) **declarando expresamente que las acepta en toda su extensión y que su capacidad no se encuentra limitada para realizar esta solicitud.**

Estas condiciones son un extracto de las *Políticas y prácticas de certificación de certificados de firma electrónica y Sello Electrónico del Sector Público,* con las normas básicas para la expedición de estos *Certificados*. Se pone a disposición del *Solicitante* la siguiente información básica y que, por razones de espacio, el deber de información quedará satisfecho con la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (DGPC) y con las Políticas y Prácticas de Certificación particulares, puestas a disposición en formato digital en el anterior enlace.

Tipo de certificado y límites de uso

La AC Sector Público expide certificados de firma electrónica para el *Personal al servicio de la Administración* y sellos electrónicos para la administración, como sistema de identificación para la actuación administrativa automatizada y para la actuación judicial automatizada, que permite autenticar documentos expedidos por dicha Administración o cualquier activo digital.

Los tipos de certificados de firma electrónica que expide AC Sector Público son:

- Certificado de Empleado Público
- Certificado con Seudónimo
- Certificado con Seudónimo de la Administración de Justicia
- Certificado de Firma Centralizada para Empleado Público

Los tipos de sello electrónico que expide AC Sector Público son:

- Certificado de Sello Electrónico

Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Estos certificados electrónicos 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 la que se deroga la directiva 1999/93/CE.

La expedición y firma de los *Certificados* se realizará por la "AC Sector Público" subordinada de la "AC Raíz" de la FNMT-RCM. La longitud de la clave utilizada en la "AC Sector Público" es de 4096 bits y en la "AC Raíz" es de 4096 bits.

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 Firma Electrónica* las diferentes competencias y funciones propias de la Administración Pública *Suscriptora* (actuando a través del personal a su servicio en calidad de *Firmante* de los *Certificados*), de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización. La FNMT-RCM y la Administración, organismos y entidades públicas podrán fijar en los acuerdos o convenios, a través del documento de relación correspondiente o, si fuera procedente, en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

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 la Ley 40/2015, y con la Ley 18/2011, de 5 de julio, 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.

Los *Certificados de firma electrónica y sello electrónico,* expedidos por la FNMT-RCM tendrán la validez establecida en sus Políticas y Prácticas de Certificación particulares, 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*.

Los *Certificados de firma electrónica y 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 de certificados de firma electrónica y Sello Electrónico del Sector Público.*

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

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 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
- No tramitar Certificados con Seudónimo, salvo 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.
- 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 de certificados de firma electrónica y Sello Electrónico del Sector Público

Obligaciones del Suscriptor y del personal al servicio de la Administración Pública (firmante)

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 referidos al cargo, puesto de trabajo, empleo o cualquier otro sea inexacto o incorrecto o no refleje o caracterice su relación, con el órgano, organismo o entidad en la que presta sus servicios; 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.

Además, la persona física asociada al *Certificado de Firma Centralizada para Empleado Público*, que actúa como *Firmante,* debe cumplir las normas de seguridad relacionadas con la custodia y uso de la contraseña de firma, como dato confidencial, personal e intransferible que garantiza el acceso a sus *Claves privadas*. Por tanto, dicho *Firmante* debe observar las siguientes cautelas relacionadas con la contraseña de firma:

- Conservar su confidencialidad, evitando comunicarlo a otras personas.
- Memorizarlo y no anotarlo en ningún documento físico ni electrónico.
- Cambiarlo en el momento en que tenga sospechas de que pueda ser conocido por otra persona.
- Notificar a la FNMT-RCM cualquier posible pérdida de control sobre su Clave privada, al objeto de revocar su Certificado de Firma Centralizada para Empleado Público y sus Claves asociadas.
- Abstenerse de escoger una contraseña fácilmente deducible de sus datos personales o predecibles (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones del mismo carácter, etc.).
- Seguir la política de seguridad de la FNMT-RCM en relación con la composición de la contraseña, periodicidad de modificación del mismo, etc.

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 —dado que es un documento publicado en la sede electrónica de la FNMT-RCM— 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, la Firma electrónica o el Sello electrónico 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 aplicables al Certificado que se verifica.
- Conocer las condiciones de utilización del Certificado conforme a las Políticas y Prácticas de Certificación.
- 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 estas Políticas y Prácticas de Certificación y en la Ley.

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 15 años, conforme a la legislación aplicable

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.

Cualificación y auditoría

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 los estándares europeos:

- ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates"
- ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons"
- 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 firma electrónica y sello electrónico que expide AC Sector Público, 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.

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

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.

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* *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, nombre y apellidos, dirección, teléfono, edad, correo electrónico, cargo, denominación o razón social.* *Datos de características personales: 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: 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)

Los interesados autorizan a la FNMT-RCM a incluir el número de serie del certificado en la lista de certificados revocados (comunicación de datos) para que sea visualizado por cualquier usuario, aunque no disponga de un certificado electrónico, tanto en el ámbito público como privado. Además, le informamos y usted consiente, que el uso del certificado a efectos de identificación o si realiza una firma electrónica, posibilita que los terceros puedan acceder a los datos que nos ha proporcionado incluidos en el certificado.

Información sobre Registros públicos de Certificate Transparency (CT).