

TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE FIRMA ELECTRÓNICA CON SEUDÓNIMO EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT-RCM)

El *Solicitante* manifiesta que, una vez descargue e instale el *Certificado de firma electrónica con seudónimo en el ámbito de la Administración de Justicia* utilizará el *Certificado* de conformidad con las condiciones adjuntas y atendiendo al contenido de *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (<https://www.sede.fnmt.gob.es/dpcs>) y en las *Políticas y Prácticas Particulares en el ámbito de las Administraciones Públicas, organismos y entidades de derecho público de la FNMT-RCM* (<https://www.sede.fnmt.gob.es/dpcs/acap>), declarando expresamente que las acepta en toda su extensión y que su capacidad no se encuentra limitada para contratar con esta Entidad

Estas condiciones son un extracto de las *Políticas y Prácticas Particulares de los Certificados de firma electrónica de Empleado 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* (<https://www.sede.fnmt.gob.es/dpcs>) y con las *Políticas y Prácticas Particulares en el ámbito de las Administraciones Públicas, organismos y entidades de derecho público de la FNMT-RCM* (<https://www.sede.fnmt.gob.es/dpcs/acap>), puestas a disposición en formato digital en el anterior enlace.

Tipo de certificado y límites de uso.

La AC Administración Pública expide certificados de firma electrónica con seudónimo para funcionarios, personal laboral, estatutario y personal autorizado al servicio de la Administración de Justicia, en el ejercicio de sus funciones para el suscriptor del certificado.

El Certificado de firma electrónica con seudónimo del personal al servicio de la Administración de Justicia, confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, y al suscriptor del certificado, que es el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

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 este personal realice 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 este tipo de certificados las diferentes competencias y funciones propias de las Administraciones Públicas suscriptoras actuando, en su caso, a través del personal a su servicio en calidad de firmante, de acuerdo con su cargo, empleo y condiciones de autorización .

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.

Las funcionalidades y propósitos del *Certificado de firma electrónica con seudónimo* permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones. La expedición y firma del *Certificado* se realizará por la "AC Administración Pública" subordinada de la "AC Raíz" de la FNMT-RCM.

Los *Certificados de firma electrónica con seudónimo* expedidos por la FNMT-RCM tendrán validez durante un periodo máximo de cinco (5) 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*.

El *Certificado de firma electrónica con seudónimo* no podrá ser utilizado 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* (<https://www.sede.fnmt.gob.es/dpcs>) y en las *Políticas y Prácticas Particulares en el ámbito de las Administraciones Públicas, organismos y entidades de derecho público de la FNMT-RCM* (<https://www.sede.fnmt.gob.es/dpcs/acap>).

La longitud de la clave utilizada en la "AC Administración Pública" es de 2048 bits y en la "AC Raíz" es de 4096 bits.

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

Obligaciones de la Entidad Suscriptora y/o el responsable de la Oficina de Registro.

La *Entidad Suscriptora* del *Certificado* y/o el *Responsable de la Oficina de Registro* tienen la obligación de:

- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una entidad diferente a la que representa como Oficina de Registro, sin perjuicio de la creación de Oficinas de Registro centralizadas o de convenios entre administraciones para efectuar registros.
- Comprobar fehacientemente los datos del Personal al servicio de la Administración de Justicia como usuario del Certificado, que actuará como Firmante del mismo, referido a su identidad y a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación de éste con la Administración, organismo o entidad a la que presta sus servicios.
- Solicitar la revocación o suspensión del Certificado del personal al servicio del órgano al que representa la Oficina de Registro cuando alguno de los datos referidos a la condición del cargo, puesto de trabajo, empleo o cualquier otro que refleje o caracterice la relación del usuario Firmante del Certificado con el órgano, organismo o entidad pública, Suscriptora del Certificado, en la que presta sus servicios, sea inexacto, incorrecto, haya variado o sea de necesaria revocación por razones de seguridad.
- En el caso de que el Certificado esté en un soporte tipo tarjeta, descargar el Certificado y sus claves directamente en la tarjeta criptográfica que se proporcione a su personal. En cualquier caso, no conservar las claves privadas asociadas a los Certificados en los equipos de la Oficina de Registro, de conformidad con las directrices de la FNMT-RCM plasmadas en los manuales de procedimiento que se entregan a las Oficinas de Registro, en las presentes Políticas de Certificación y Prácticas de Certificación Particulares y en la DGPC

Obligaciones del personal al servicio de la Administración Pública.

El personal al servicio de la Administración de Justicia, como Firmante del Certificado y sus Claves, tiene 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 de Justicia.
- Comunicar al Responsable de la Oficina de Registro, la pérdida, extravío, o sospecha de ello, de la tarjeta o soporte del Certificado del que es usuario y custodia, con el fin de iniciar, en su caso, los trámites de su revocación.

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

Cualquier tercera parte que confía de manera razonable en un certificado, tendrá qué:

- Asegurar que la confianza en los certificados emitidos bajo la política de certificación está restringida a los usos apropiados (véase el documento Política y Prácticas de Certificación Particulares de Certificados de Empleado Público).
- Verificar la validez del certificado, asegurándose de que no ha caducado.
- Asegurarse de que el certificado no ha sido suspendido o revocado, accediendo a la información sobre el estado actual de revocación, disponible en la ubicación especificada en el propio certificado.
- Determinar que dicho certificado ofrece garantías suficientes para el uso previsto.

Limitaciones de responsabilidad

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 las correspondientes Políticas y Prácticas de Certificación. En ningún caso será responsable de las acciones o de las pérdidas en las que incurran, solicitantes, titulares, entidades usuarias o, en su caso, terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los correspondientes procedimientos de expedición y/o de gestión de los certificados.

La FNMT-RCM no responderá en los supuestos de caso fortuito, 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.

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 la Declaración de Prácticas de Certificación y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

En todo caso y con la condición de cláusula penal, la cuantía que la FNMT - RCM debiera satisfacer, en concepto de daños y perjuicios, por imperativo judicial a terceros perjudicados o miembros de la Comunidad Electrónica en cualquier ámbito de actuación público o privado, en defecto de regulación específica en los contratos o convenios, se limita a un máximo de SEIS MIL EUROS (6.000 euros).

En caso de terminación de la actividad del Prestador de Servicios de Confianza, 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 Confianza 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 disputa

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 RD 1.114/1999, de 25 de junio (BOE nº 161 de 7 de julio).

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.

Licencias y repositorio, marcas confiables y auditoría

La FNMT-RCM cuenta con una larga trayectoria histórica en la realización de sus actividades industriales, así como el respaldo del Estado, como Entidad Pública Empresarial adscrita al Ministerio de Hacienda y Función Pública. 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, ha contribuido a impulsar la extensión de los servicios a los que ha sido facultada y ha obtenido el reconocimiento del entorno privado en el sector de la certificación electrónica y las redes telemáticas abiertas, alcanzando un destacado puesto en la prestación de los servicios de certificación.

La FNMT - RCM, como Prestador de Servicios de Confianza, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplica especialmente a este tipo de certificado la siguiente:

- Expedición y administración de certificados electrónicos cualificados de conformidad con 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 con seudónimo en el ámbito de la Administración de Justicia, son cualificados conforme al Reglamento (UE) N° 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

PROTECCION DE DATOS

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, le informamos que los datos que nos proporcione se incorporarán a un fichero de datos de carácter personal cuyo responsable es la FNMT-RCM. Su estructura y finalidad son las previstas en el número 5 del Anexo a la Orden EHA/2357/2008, por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (BOE 190, de 7 de agosto) o norma que la sustituya. La información existente en el citado fichero está destinada a la prestación de servicios electrónicos, informáticos y telemáticos para el sector público y privado.

Los interesados podrán ejercitar los derechos de acceso, rectificación, cancelación y, en su caso, oposición ante el responsable del fichero (FNMT-RCM) remitiendo un escrito, adjuntando una fotocopia de su DNI o autorizándonos la consulta al Sistema de Verificación de Datos de Identidad. También puede ejercitar sus derechos a través del Registro Electrónico (<https://www.sede.fnmt.gob.es/tramites>) utilizando el "Formulario de propósito general". El domicilio de esta Entidad es calle Jorge Juan nº 106, 28009 - Madrid. 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. Todo ello, a los efectos del necesario conocimiento por terceros del propósito y estado del certificado expedido o de la firma realizada, de conformidad con el art. 11.2.c) de la LOPD.