TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE FIRMA ELECTRÓNICA CENTRALIZADA PARA EMPLEADO PÚBLICO DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA (FNMT-RCM).

El *Solicitante* manifiesta que, una vez generadas las credenciales de su identidad y el *Certificado de Firma Electrónica Centralizada para Empleado Público* 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 **y en la** Declaración de prácticas y políticas de certificación de certificados de firma electrónica centralizada para empleados públicos (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 realizar esta solicitud.**

Estas condiciones son un extracto de la *Declaración de prácticas y políticas de certificación de certificados de firma electrónica centralizada para empleados públicos,* 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 *Declaración de prácticas y políticas de certificación de certificados de firma electrónica centralizada para empleados públicos*, 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 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 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.

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, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

El *Certificado* de firma electrónica centralizada para empleados públicos es un tipo de certificado orientado a la realización de firmas a distancia o en servidor, esto es, la generación de las *Claves pública y privada* no se realiza directamente en el navegador de Internet del *Firmante* o en otro dispositivo en su poder, y tampoco se descarga su *Certificado*, sino que se generan y se almacenan en un entorno seguro perteneciente a la FNMT-RCM. 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*.

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 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, normativa o convenios, a través del documento de relación correspondiente o en la Ley de Emisión de estos Certificados, otros escenarios de uso adicionales. Estos certificados podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones, organismos y entidades públicas cuando estas lo admitan según los acuerdos, convenios o la normativa que le sea de aplicación.

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 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 Administración Pública" subordinada de la "AC Raíz" de la FNMT-RCM.

Los *Certificado de firma electrónica centralizada para empleado público* expedidos por la FNMT-RCM 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*.

El *Certificado de firma electrónica centralizada para empleado público* 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* y en las *Políticas* y *Prácticas Particulares en el ámbito de las Administraciones Públicas, organismo y entidades de derecho público.*

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

Las Oficinas de Registro, dependientes de la Autoridad de Registro de la FNMT – RCM, tienen la obligación de:

- Comprobar fehacientemente la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto en la *Declaración de Prácticas y Políticas de Certificación*.
- Informar a los usuarios de los Certificados sobre su adecuado uso, de conformidad con estos términos, las Declaraciones de Prácticas y Políticas de Certificación y la normativa aplicable
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante el plazo de tiempo establecido en la legislación vigente.
- Permitir a la FNMT-RCM el acceso a los archivos y la auditoría de sus procedimientos en relación con los datos obtenidos en calidad de *Oficina de Registro*.
- Informar a la FNMT-RCM de cualquier aspecto que afecte a los *Certificados* expedidos por dicha Entidad (ej.: solicitudes de expedición, renovación…).
- Comunicar a la FNMT-RCM de forma diligente las solicitudes de expedición de *Certificados*.
- Respecto de la extinción de la validez de los Certificados:
  1. Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.
  2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación de los *Certificados*.
- Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la *Declaración de Prácticas y Políticas de Certificación*.
- Las *Oficinas de Registro*, a través del personal adscrito al servicio por relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM.

Obligaciones del personal al servicio de la Administración Pública

La persona física asociada al *Certificado*, que actúa como *Firmante* debe cumplir las normas de seguridad relacionadas con la custodia y uso del PIN, como dato confidencial, personal e intransferible que garantiza el acceso a sus *Claves privadas*. Por tanto, el Titular debe observar las siguientes cautelas relacionadas con el PIN:

- 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 y sus Claves asociadas.
- Abstenerse de escoger un PIN 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 del PIN, 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 la Declaración de Prácticas y Políticas 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 la Declaración de Prácticas y Políticas 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 la Declaración de Prácticas y Políticas 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 la Declaración de Prácticas y Políticas 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 esta Declaración de Prácticas de Certificación y en la Ley.

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 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.

Cualificación 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 aplican especialmente a estos tipos de certificados las siguientes:

- 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” y ETSI EN 319 412-2 “Certificate profile for certificates issued to natural 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 Certificado de firma electrónica centralizada para empleado 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

PROTECCIÓN DE DATOS.

Le ofrecemos información básica sobre los datos de carácter personal que estamos recogiendo. 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 según las recomendaciones de la Agencia Española de Protección de Datos. 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. Una vez finalizada su relación con la FNMT-RCM mantendremos sus datos bloqueados para el ejercicio de derechos.*
LEGITIMACIÓN	*La base jurídica para el tratamiento de sus datos es la necesidad de gestionarlos para realizar la prestación como tercera parte de confianza.*
DESTINATARIOS	*Se comunicará su nº de serie del certificado a terceros con el fin de que puedan comprobar su validez y lo datos que consten en el certificado cuando lo utilice. 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 http://www.fnmt.es/rgpd (PÁGINA PRINCIPAL)*
PROCEDENCIA	*Consentimiento inequívoco del interesado. De organizaciones donde prestan servicios los afectados (representantes, apoderados o contactos)*
MEDIDAS DE SEGURIDAD	*Esquema Nacional de Seguridad. Más información en enlace inferior.*
CATEGORÍA DE DATOS	*Datos identificativos, de características personales y circunstancias sociales, según se explica en la información adicional del Registro de Actividades del enlace inferior.*

Puede consultar información adicional y detallada sobre este tratamiento en:

http://www.fnmt.es/rgpd (TRATAMIENTO Nº 15)

Los interesados podrán ejercitar los derechos de acceso, rectificación, cancelación y, en su caso, oposición ante la 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.

Información sobre Registros públicos de Certificate Transparency (CT).