

PRESTADOR DEL SERVICIO DE CERTIFICACION DEL CORPME

CERTIFICADO CUALIFICADO DE ADMINISTRACIÓN LOCAL LICENCIA DE USO

En, a dede 20.....

D./Dña., con
DNI/NIF/Pasaporte/NIE nº, correo electrónico, número
de teléfono, representando a la administración local
..... con NIF nº, de
la provincia y la unidad local, con
cargo administrativo

SOLICITUD: El titular declara que ha generado en un dispositivo criptográfico seguro una clave privada y que solicita al CORPME la emisión de un **Certificado Cualificado de Administración Local** y que se compromete a utilizarlo de acuerdo con lo dispuesto en la Declaración de Prácticas de Certificación y en la Política de Certificación de Certificados Externos del CORPME¹. Asimismo, **solicita la revocación de todos los Certificados Cualificados de Administración Local** a su nombre que existieran con anterioridad a la emisión del certificado objeto de este documento.

ACEPTACION: El titular declara que ha recibido el certificado, aceptando que cada firma digital creada mediante la clave privada correspondiente a la clave pública certificada es su firma electrónica y que conoce que el uso de la clave privada certificada es personal e intransferible, asumiendo la responsabilidad por el mal uso de la misma, así como los perjuicios que de éste pudieran derivarse. También acepta las limitaciones de uso correspondientes, y manifiesta que no utilizará la clave privada para emitir certificados de clave pública o listas de certificados revocados.

D./Dña.,

Responsable de la Unidad de Tramitación.....

CERTIFICACION: Certifica que, en su presencia, el titular ha generado en un dispositivo criptográfico seguro una clave privada y que ha recibido por parte del CORPME el correspondiente **Certificado Cualificado de Administración Local**, todo ello de acuerdo con lo dispuesto en la Política de Certificación de Certificados Externos y en la Declaración de Prácticas de Certificación del CORPME.

Fdo.: El titular

Fdo.: El Responsable de la Unidad de Tramitación

Información básica sobre Protección de Datos:

Responsable del tratamiento: CORPME.

Finalidad del tratamiento: Gestión de la solicitud realizada por el usuario, ejecución del convenio suscrito y/o prestación del servicio de firma electrónica; en base a lo indicado en la información adicional que referencia más adelante.

Legitimación: Contrato y/o prestación del servicio de firma electrónica.

Destinatarios: No está prevista la comunicación de sus datos personales salvo cuando sea necesario para dar cumplimiento a obligaciones legales o fuera necesaria para la ejecución del contrato o convenio suscrito en su caso.

Derechos: Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.

Información adicional: Puede consultar información adicional y detallada sobre protección de datos en las condiciones de protección de datos del presente documento.

¹ La Declaración de Prácticas de Certificación y la Política de Certificación, se podrá consultar en la dirección: <http://pki.registradores.org/normativa/index.htm>

TÉRMINOS Y CONDICIONES DE CERTIFICACIÓN Y DECLARACIÓN DE DIVULGACIÓN

El presente documento constituye un extracto de los derechos y obligaciones contenidos en la Declaración de Prácticas de Certificación (en adelante, DPC) del Colegio de Registradores de la Propiedad y Mercantiles de España (en adelante CORPME) y aplica a los **Certificados Cualificados de Administración Local**. Estos Términos y Condiciones desarrollan y completan lo dispuesto en la DPC y Políticas de Certificación (en adelante, PC's) publicadas.

Los efectos legales de un certificado, así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la legislación vigente, la DPC y a la PC de Certificados Externos en la versión obrante en cada momento en la siguiente URL: <http://pki.registradores.org/normativa/index.htm>.

Antes de solicitar un certificado o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer los presentes Términos y Condiciones, al objeto de valorar adecuadamente la confianza que ofrece un certificado. No se podrá alegar la ignorancia de estos Términos y Condiciones para eximirse de las responsabilidades propias ni para exigir las a otra parte.

1. Información de contacto del Prestador de Servicios de Confianza

Colegio de Registradores de la Propiedad y Mercantiles de España.

Prestador del Servicio de Certificación del CORPME.

C/ DIEGO DE LEON, 21.

28006-MADRID

Teléfono: 902181442 / 912701699

Email: psc@registradores.org

Web: <http://pki.registradores.org/normativa/index.htm>

2. Tipo de certificado, procedimientos de validación y uso

Los **Certificados Cualificados de Administración Local** son certificados de uso intransferible que acreditan la identidad de su titular, así como su condición de personal adscrito a la administración local. Se emiten para el exclusivo uso en el ámbito de su actividad, en la relación con los Registros de España y con otras Administraciones Públicas. Tienen como finalidad principal la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. También pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y para la firma de correos electrónicos.

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.

Los **Certificados Cualificados de Administración Local** se rigen por las políticas de certificación de la normativa ETSI EN 319 411-2, referentes a QCP-n-qscd.

Estos certificados se emiten bajo la política con OID 1.3.6.1.4.1.17276.0.2.4.2 descrita en la PC de Certificados Externos.

3. Límites de uso

Los **Certificados Cualificados de Administración Local** no podrán ser utilizados cuando expire su periodo de validez, cuando sea solicitada su revocación o cuando se cumpla alguna de las causas de extinción de la vigencia establecidas en la DPC y en la PC de Certificados Externos.

Los usuarios de un certificado pueden comprobar la validez del mismo en el Servicio de Validación de Certificados, a través de la dirección donde tiene disponible su OCSP.

También se publica un directorio que contiene las Listas de Certificados Revocados (en adelante, CRL's), firmadas por el Prestador del Servicio de Certificación (en adelante, PSC) y que se actualizan cada vez que se revoca un certificado.

No se considerarán válidas las firmas electrónicas recibidas fuera del periodo de vigencia del certificado, salvo cuando se acredite que la firma fue realizada dentro de este, mediante un sello de tiempo de los Registros o de otro sistema de sellado de tiempo reconocido por el PSC del CORPME.

Antes de dar por válida una firma electrónica será preciso verificar que el certificado que la respalda no ha sido revocado, pudiéndolo comprobar a través del Servicio de Validación de Certificados, a través de la dirección donde tiene disponible su OCSP, o a través del directorio que contiene las CRL's.

Los certificados están firmados electrónicamente por el PSC del CORPME con la clave privada correspondiente a la clase de los certificados externos y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 2048 bits, y su periodo de vigencia es de dos (2) años.

Las licencias de uso, solicitudes de revocación, certificaciones acreditativas de atributos certificables, y en general cualesquiera documentos firmados de los que se deriven derechos y obligaciones para los intervinientes

en el PSC del CORPME, así como los registros de auditoría asociados, se almacenarán durante un periodo mínimo de quince (15) años.

El CORPME utilizará diferentes sistemas para emitir y revocar certificados, proporcionando alta disponibilidad al servicio. Además, el servicio de información del estado de certificados, en sus dos variantes (CRL's y OCSP), está disponible 24 horas todos los días del año, tanto para los terceros que confían como para los titulares de los certificados u otras partes que los requieran.

4. Renovación

Desde los sistemas del CORPME se notificará al titular al correo electrónico que facilitó, la futura expiración de los certificados, con al menos dos (2) meses de antelación a la fecha en que se produzca, indicando al titular los pasos a seguir para la obtención de un nuevo certificado, de acuerdo al procedimiento establecido en la DPC.

5. Revocación

La revocación de un certificado supone su total pérdida de validez y la exención de responsabilidad del PSC por cualquier daño producido como consecuencia del uso del certificado revocado con posterioridad a su revocación.

La revocación producirá efectos frente al solicitante desde el momento en que entregue la correspondiente solicitud a la Unidad de Tramitación y, frente a terceros, desde que sea publicada en el Directorio de Listas de Revocación. Será obligación del titular comprobar si la revocación del certificado ha sido publicada en el Directorio de Listas de Revocación http://pki.registradores.org/crls/crl_ext_psc_corpme.crl.

Para solicitar la revocación del certificado de forma presencial el titular deberá personarse ante la Unidad de Tramitación que emitió el certificado o, en caso de urgencia, en cualquier otra Unidad de Tramitación del CORPME. El Responsable de la Unidad de Tramitación comprobará la identidad del solicitante y procederá a la revocación del certificado, guardando la solicitud de revocación firmada por ambos durante quince (15) años.

Adicionalmente, podrá solicitarse la revocación de los certificados firmando una solicitud electrónica, como así queda recogido en la DPC del CORPME. La Unidad de Tramitación Central procederá a la revocación del certificado y notificará al titular la confirmación del estado de revocación. La dirección web para acceder a este servicio de revocación on-line es <https://pki.registradores.org/rauserrevocserver/>.

La Junta de Gobierno podrá ordenar a la Unidad de Tramitación Central la revocación de un certificado, sin perjuicio de las responsabilidades en que por ello pudiera incurrir ante su titular. La orden indicará el plazo en el que debe procederse a la revocación. La Unidad de Tramitación notificará de forma inmediata al titular por correo electrónico y por un medio fehaciente, y procederá a la revocación en el momento ordenado.

Los servicios prestados ponen a disposición del usuario un servicio de Lista de Revocación de Certificados (CRL), basado en lo establecido en el ITU-T X.509 y un servicio de Verificación Online del Estado de los Certificados (OCSP), basado en lo establecido en la IETF RFC 6960. Ambos servicios se complementan y están configurados de tal forma que se da cumplimiento al estándar ETSI EN 319 411-2. La información sobre la revocación está disponible on-line 24 horas todos los días del año, tanto para los terceros que confían como para los titulares de los certificados u otras partes que los requieran. La información sobre la revocación se mantendrá hasta la fecha de expiración del certificado. En caso de compromiso de la clave privada concerniente a la CA del certificado o en caso de terminación de servicios de CA, el CORPME pondrá a disposición tanto para los terceros que confían como para los titulares de los certificados u otras partes que los requieran la información de revocación hasta que todos los certificados concernidos hayan expirado.

6. Obligaciones del titular del certificado

El **Certificado Cualificado de Administración Local** debe ser utilizado de acuerdo con las finalidades propias del mismo, así como con lo establecido en la legislación española, en la DPC y en las PC's publicadas.

En particular, son obligaciones del titular:

- Suministrar a las Unidades de Tramitación información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
- Informar a los responsables de PKI de CORPME de cualquier modificación de esta información.
- Conocer, aceptar y firmar la licencia de uso del certificado.
- Utilizar el certificado exclusivamente para los usos especificados en estas Términos y Condiciones y en el propio certificado, y únicamente dentro de su periodo de vigencia.
- Proteger y almacenar sus claves criptográficas privadas de forma confidencial e inaccesible a terceros no autorizados, adoptando las medidas de seguridad necesarias para conservarlas.
- Mantener el secreto de la contraseña que protege su clave privada, así como del código que permite revocar el certificado.
- Notificar inmediatamente a la Unidad de Tramitación correspondiente la pérdida o divulgación de la clave privada, o cualquier situación que pueda afectar a la validez del certificado, solicitando su revocación, conforme a los procedimientos previstos en la DPC y PC's publicadas.

- Abstenerse de utilizar la clave privada del certificado desde el mismo momento en el que se solicita o es advertido por la Autoridad de Certificación (en adelante, CA) o la Autoridad de Registro (en adelante, RA) de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.
- Abstenerse de utilizar la clave privada del certificado desde el mismo momento en el que se notifica o advierte el compromiso de la misma.
- Destruir el certificado cuando así lo exija la CA, en virtud del derecho de propiedad que en todo caso conserva sobre el mismo y cuando el certificado caduque o sea revocado.
- No monitorizar, manipular o realizar actos de “ingeniería inversa” sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la CA.
- No transferir ni delegar sus responsabilidades sobre un certificado que le haya sido asignado a un tercero.
- Instalar el certificado únicamente en servidores que sean accesibles a los subjectAltName(s) enumerados en el perfil del certificado.
- Responder a las instrucciones de la CA en relación con el compromiso de la clave o el uso indebido del certificado dentro de un periodo de tiempo especificado.
- Reconocer y aceptar que la CA tiene derecho a revocar inmediatamente si el solicitante viola los Términos y Condiciones o si descubre que el certificado está siendo usado en actividades criminales, como fraude o distribución de malware.
- Crear todas las firmas digitales haciendo uso del DSCF en el que se generan las claves pública y privada del certificado y que es entregado al suscriptor en el momento de la emisión.

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

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

- Verificar, antes de depositar su confianza en un certificado, que el mismo está vigente y no ha sido revocado. A tal fin deberá comprobar la validez y vigencia del certificado de firma por alguno de los medios disponibles: consulta de las CRL's o consulta en línea de estado de certificados mediante protocolo OCSP, antes de aceptar cualquier comunicación o documento firmado digitalmente con uno de los certificados emitidos por el CORPME.
- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la PC correspondiente.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía, asegurándose de que no han caducado.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.

8. Limitaciones de responsabilidad

El PSC no responderá, en ningún caso, de la utilización que los titulares hagan de los certificados, ni de los errores de hecho o de interpretación que puedan cometer quienes validen una firma. En particular, el PSC no tendrá responsabilidad alguna por:

- Los daños y perjuicios, directos o indirectos, causados por la utilización de los certificados y de las claves certificadas para usos no permitidos o fuera de su período de vigencia, así como por la pérdida o divulgación de la clave privada del titular.
- El contenido de los documentos firmados con una firma digital basada en un certificado emitido por él, ni por la información contenida en un servidor por él certificado
- Los fallos o errores debidos a los equipos informáticos, navegadores o aplicaciones utilizados por el titular o por los terceros usuarios de los certificados.

9. Acuerdos aplicables y Declaración de Prácticas y Políticas de Certificación

Los documentos de DPC y de PC de Certificados Externos, publicados en la dirección <http://pki.registradores.org/normativa/index.htm>, recogen la información pública de los Términos y Condiciones y características de los servicios de certificación y servicios de expedición de certificados electrónicos por parte del CORPME como PSC, incluyendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición del **Certificado Cualificado de Administración Local**.

Las actividades que el CORPME pueda subcontratar para llevar a cabo su actividad como PSC se desarrollan según lo establecido en su DPC y en los contratos y acuerdos formalizados con las entidades que realizan tales actividades. En estos casos, el acceso a la información propiedad del CORPME por parte de terceros sigue el protocolo definido en la Política de Seguridad de esta entidad, en cuanto a la identificación de riesgos, establecimiento de controles de seguridad para proteger el acceso a la información y la formalización de los corres-

pondientes acuerdos de confidencialidad y, si procede, el contrato para el tratamiento de datos de carácter personal en cumplimiento de la normativa vigente.

10. Política de privacidad

De acuerdo con el Reglamento General de Protección de Datos (REGLAMENTO UE 2016/679), el usuario y titular de los datos queda informado que el Responsable del tratamiento de sus datos personales es el **COLEGIO DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA** (en adelante, "CORPME"), con CIF: Q-2863012-G y Sede Colegial en la Calle Diego de León, 21, 28006 de Madrid.

El tratamiento de sus datos personales se realizará por el CORPME para las siguientes finalidades en base al tipo de documento suscrito por el usuario:

- Para licencias de uso: finalidad de tramitar la solicitud presentada y la correspondiente facturación.
- Para revocaciones: la finalidad del tratamiento es gestionar la solicitud de revocación del Certificado.
- Para delegación de funciones: la finalidad del tratamiento es la gestión de solicitudes y emisión de certificados digitales en cumplimiento de las finalidades recogidas en la declaración de prácticas de certificación del Colegio de Registradores en calidad de prestador de servicios de certificación.
- Declaración Responsable de Roles de Confianza: la finalidad del tratamiento es la gestión y tramitación de su Declaración de condición de Responsable.
- La declaración de registrador – empleados registro: finalidad de gestionarla Declaración del Registrador y la expedición de su Certificado.

La base legitimadora que habilita para el tratamiento de sus datos es la propia ejecución del servicio o contrato solicitado por el interesado o cumplimiento del convenio suscrito en su caso.

Asimismo, se informa al usuario que sus datos serán cedidos únicamente para el cumplimiento de las obligaciones establecidas legalmente o fuera necesaria para la ejecución del contrato o convenio suscrito en su caso. Los datos personales solicitados en el formulario son esenciales para la gestión de la solicitud realizada por el usuario, la ejecución del convenio suscrito y/o prestación del servicio de firma electrónica, de tal forma que la negativa a suministrarlos supondrá la imposibilidad de su realización. El titular de los datos garantiza que los datos personales son reales y veraces.

No está prevista la comunicación de sus datos personales por el CORPME, sin perjuicio de aquellas comunicaciones que puedan ser realizadas para dar cumplimiento a las obligaciones y responsabilidades impuestas por las leyes o normas de obligado cumplimiento, o cuando fuera requerida para ello por mandato de autoridad competente con arreglo a Derecho o como requisito necesario para la suscripción del contrato solicitado.

Le informamos de la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos. Del mismo modo, el usuario podrá reclamar ante la Agencia Española de Protección de Datos (AEPD) www.agpd.es.

Puede obtener más información sobre el tratamiento de datos personales realizados por el CORPME en las políticas de protección de datos disponibles en la web: www.registradores.org

El periodo máximo de conservación de los datos será de 15 años. En todo caso, el CORPME podrá conservar los datos de los titulares por un tiempo superior en aquellos supuestos en que sea necesario por la existencia de responsabilidades derivadas de la prestación servicio.

Los interesados podrán ponerse en contacto con el Delegado de Protección de Datos del CORPME a través del correo electrónico dpo@corpme.es.

11. Política de devolución

No aplicable.

12. Ley aplicable, quejas y resolución de disputa

Las operaciones y funcionamiento del PSC del CORPME, así como la DPC y las PC's que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Reglamento UE 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- 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, así como la legislación española aplicable en materia de protección de datos de carácter personal.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Todas las reclamaciones entre usuarios y CORPME deberán ser comunicadas por la parte en disputa al CORPME, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a la prestación de servicios de certificación, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales españoles, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

13. Licencias y repositorio, marcas confiables y auditoría

El CORPME, como PSC, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplican especialmente a este tipo de certificado 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”.

Puede comprobarse la inclusión de los certificados cualificados expedidos por el CORPME en la lista de prestadores de servicios de confianza (TSL) de España y de la Unión Europea, a través de los siguientes enlaces:

<https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/ES/12>

Asimismo, el CORPME está registrado como prestador cualificado en el Ministerio de Asuntos Económicos y Transformación Digital:

<https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

<https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx>

Las fuentes de información anteriores, tal como lo define RFC 5280, se establecen como el Trust Anchor, que es el punto final de un proceso de validación de certificados. En los Trust Anchor se garantiza la identidad digital del servicio identificado en las entradas de los servicios de confianza tal y como se define en ETSI TS 119 61.

Conforme a lo establecido en el Reglamento UE nº 910/2014, el CORPME realizará auditorías bienales de conformidad con dicho Reglamento.