



**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HAN DE REGIR EL CONTRATO DE SERVICIOS DENOMINADO
“SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA”, A ADJUDICAR POR PROCEDIMIENTO
SIMPLIFICADO ORDINARIO, MEDIANTE PLURALIDAD DE CRITERIOS**

CLÁUSULA 1.-	INTRODUCCIÓN	3
CLÁUSULA 2.-	OBJETO	3
CLÁUSULA 3.-	AMBITO	4
CLÁUSULA 4.-	DESCRIPCIÓN DE LOS SERVICIOS.....	4
4.1	Consideraciones generales.	4
4.2	Servicio de emisión, renovación, revocación y suspensión de certificados electrónicos.	5
4.2.1	Certificados electrónicos reconocidos para las Administraciones Públicas.	5
4.2.2	Otros certificados electrónicos reconocidos.	5
4.2.3	Certificados electrónicos de componente.	5
4.3	Servicio de emisión de soportes criptográficos.	6
4.4	Servicio de consulta de validez de los certificados.	6
4.5	Servicio de renovación de certificados en tarjeta criptográfica por el usuario.	7
4.6	Servicio de sellado de tiempo o de fechado digital.	7
4.7	Servicio de información y seguimiento de certificados emitidos.	7
4.8	Servicio de registro de usuarios.	8
4.9	Servicio de atención y soporte a registradores.	10
4.10	Servicios bajo demanda.	10
CLÁUSULA 5.-	FASES DE EJECUCIÓN DEL SERVICIO	11
5.1	Fase de Puesta en Marcha del Servicio	11
5.2	Fase de Pleno Servicio	11
5.3	Transición de Salida	12
CLÁUSULA 6.-	ACUERDOS DE NIVEL DE SERVICIO	12
6.1	Niveles de servicio.	12
6.1.1	Prestación del servicio.	12
6.1.2	Resolución de incidencias y disponibilidad del servicio.	12
6.2	Cálculo de penalizaciones	13
6.2.1	Prestación del servicio.	13
6.2.2	Resolución de incidencias y disponibilidad del servicio.	14
CLÁUSULA 7.-	EQUIPO ADSCRITO A LA PRESTACIÓN DEL SERVICIO	14
7.1	Responsable del Servicio ante ICM	15
7.2	Equipo de registradores de la Oficina de registro móvil	15
7.3	Jefe de Proyecto para soporte a proyectos.	16
CLÁUSULA 8.-	MODELO DE SEGUIMIENTO DE LA EJECUCIÓN DEL CONTRATO	16
8.1	Comité de seguimiento del contrato	16
8.2	Comité operativo	17



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1000031128665707605074**





8.3	Informes de Seguimiento del Servicio	18
8.4	Modelo de Gestión de Atención de Incidencias y Soporte técnico	19
CLÁUSULA 9.-	PLAZO DE GARANTÍA.....	19
CLÁUSULA 10.-	GESTION DE LA SEGURIDAD	20
10.1	Documentación de seguridad	21
10.2	Usuarios de sistemas de información.....	22
10.3	Protección de datos de carácter personal.	22
10.4	Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica	26
10.5	Medidas de seguridad y compromisos del adjudicatario en el caso de acceso remoto a infraestructuras de ICM	27
10.6	Propiedad de los trabajos	28
10.7	Sigilo y Confidencialidad de la información tratada.....	29
10.8	Restricciones generales	30
10.9	Auditoría de la seguridad y trazabilidad de los servicios.....	30
CLÁUSULA 11.-	PLAZO DE EJECUCIÓN.....	31
CLÁUSULA 12.-	DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE ICM	31
CLÁUSULA 13.-	PRESUPUESTO BASE DE LICITACIÓN.....	32
13.1	Servicios de Coste Fijo.....	32
13.2	Servicios de Coste Variable.....	32
CLÁUSULA 14.-	CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS	34



CLÁUSULA 1.- INTRODUCCIÓN

El desarrollo de la Sociedad de la Información y la difusión de los efectos positivos que de ella se derivan, exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas.

Con la finalidad de ofrecer respuesta a esta necesidad han surgido los **sistemas de certificación electrónica**, que permiten garantizar la procedencia, el momento y la integridad de los mensajes intercambiados a través de redes de telecomunicaciones.

A ellos se refiere la **Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos**, que establece el derecho de los ciudadanos a comunicarse con las diferentes Administraciones Públicas a través de medios telemáticos. Dispone esta Ley que este derecho ha de estar ligado a la implementación, en el ámbito de las Administraciones Públicas y sus organismos y entidades vinculados o dependientes, de las infraestructuras y nuevos sistemas electrónicos, informáticos y telemáticos previstos en la referida normativa. En particular, dispone el artículo 13 que las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

- a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente, que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.
- b) Sistemas de firma electrónica para la actuación administrativa automatizada.
- c) Firma electrónica del personal al servicio de las Administraciones Públicas.
- d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Asimismo, hay que tener en cuenta lo dispuesto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.

Por tanto, la utilización por parte de la Administración de la Comunidad de Madrid de los diferentes sistemas de certificación electrónica resulta clave para conseguir el objetivo de garantizar el derecho de los ciudadanos de la Comunidad de Madrid a relacionarse de forma segura por medios telemáticos con la Administración.

La prestación de los servicios cuya contratación se pretende, requieren una disponibilidad tal que sólo pueden ser realizados por empresas que tengan la condición de Prestadores de Servicios de Certificación, (Autoridad de Certificación), especializadas en la materia, y que posean el equipamiento, infraestructura, tecnología y conocimientos necesarios para llevarlos a cabo con medios propios.

CLÁUSULA 2.- OBJETO

Es objeto del presente contrato la prestación de los **servicios técnicos, administrativos y de seguridad de los sistemas de certificación electrónica** necesarios en orden a garantizar la validez y eficacia de la emisión





y recepción de comunicaciones y documentos producidos a través de técnicas y medios telemáticos en el ámbito de actuación de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (en adelante ICM).

CLÁUSULA 3.- AMBITO

Los servicios de certificación electrónica que constituyen el objeto del contrato, se prestarán a ICM para su implantación en la Administración General de la Comunidad de Madrid e ICM.

CLÁUSULA 4.- DESCRIPCIÓN DE LOS SERVICIOS

4.1 Consideraciones generales.

En la prestación de los servicios objeto del contrato, se observarán los siguientes requisitos generales:

- Los licitadores deberán tener la condición de Prestador de Servicios de Certificación y, como tal, deberán haber realizado la comunicación al Ministerio de Industria, Energía y Turismo, prevista en el apartado 2 del artículo 30 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

A tal efecto, deberán aportar, en el Sobre nº 1 "Documentación Administrativa", la documentación acreditativa del cumplimiento de dicha obligación.

- Los certificados deberán cumplir la recomendación de la Unión Internacional de Telecomunicaciones (UIT) X.509 V3 o superiores (ISO/IEC 9594-8 de 1997) o aquellas otras que pudieran ser publicadas en el "Diario Oficial de la Unión Europea", de conformidad con lo previsto por la legislación de firma electrónica,
- El contratista estará sujeto, en la ejecución del contrato, al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- El contratista estará sujeto, en la ejecución del contrato, al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- El contratista estará sujeto al Esquema de Identificación y Firma Electrónica de la Administración General del Estado.
- El contratista deberá disponer de la Declaración de Prácticas de Certificación exigida en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que deberá estar disponible de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita, de conformidad con lo establecido en el citado artículo. Los licitadores deberá aportar en el **Sobre nº 2 "Documentación Técnica"**, la Declaración de Prácticas de Certificación, de conformidad con lo establecido en el Apartado 6 del Anexo I del Pliego de Cláusulas Jurídicas.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1000031128665707605074**



4.2 Servicio de emisión, renovación, revocación y suspensión de certificados electrónicos.

4.2.1 Certificados electrónicos reconocidos para las Administraciones Públicas.

Se contemplarán los siguientes tipos de *certificados electrónicos* para las Administraciones Públicas según lo establecido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente dicha ley, y *reconocidos* según la Ley 59/2003, de 19 de diciembre, de firma electrónica:

- Certificados para la identificación electrónica de las **sedes electrónicas** de la Comunidad de Madrid. Estos certificados se podrán emitir, a petición de ICM, tanto en software como en hardware. La validez de estos certificados será de 3 años.
- Certificados de **sello electrónico para la actuación administrativa automatizada**. Estos certificados se podrán emitir, a petición de ICM, tanto en software como en hardware. La validez de estos certificados será de 3 años.
- Certificados para el **personal al servicio de las Administraciones Públicas**. Estos certificados se podrán emitir, a petición de ICM, tanto en software como sobre tarjetas criptográficas personalizadas, homologadas al efecto por ICM, con independencia de que sean o no suministradas al amparo de este contrato. La validez de estos certificados será de 3 años.

4.2.2 Otros certificados electrónicos reconocidos.

Se contemplarán los siguientes tipos de certificados electrónicos reconocidos según lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica:

- Certificados de **persona jurídica** para administradores, representantes legales y voluntarios con poder bastante a esos efectos. Estos certificados se podrán emitir, a petición de ICM, tanto en software como sobre tarjetas criptográficas personalizadas. La validez de estos certificados será de 2 años.
- Certificados de **persona física** para el ciudadano que se relacione con la Administración Pública, a petición de cualquier persona física con domicilio en la Comunidad de Madrid, en adelante certificado de **ciudadano**. La validez de estos certificados será de al menos 3 años.

4.2.3 Certificados electrónicos de componente.

Se contemplarán los siguientes tipos de certificados electrónicos:

- Certificados de **Servidor Seguro**, que permitirán establecer comunicaciones seguras con los clientes utilizando la tecnología SSL/TLS garantizando la integridad y confidencialidad de las comunicaciones, en sus distintas modalidades: monodominio SSL y SSL EV (Extended Validation), todos los subdominios asociados a un dominio principal (wildcard), o multidominio (SAN). La validez de estos certificados será de 3 años.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1000031128665707605074**

- Certificados de **Firma de Código**, que garantizará la identidad del autor y la integridad del contenido de software. La validez de estos certificados será de 3 años
- Certificados de **Sello de Entidad o sello de empresa**, que permitirán identificar y autenticar máquinas o aplicaciones, e Intercambiar mensajes cifrados y/o firmados con garantías de confidencialidad, autenticación e integridad. La validez de estos certificados será de 3 años

Los certificados incluidos en este apartado se generarán, a petición de ICM tanto en software como en dispositivos seguros de creación de firma como tarjetas criptográficas o dispositivos hardware (Hardware Security Module - **HSM**).

4.3 Servicio de emisión de soportes criptográficos.

El adjudicatario deberá proporcionar un servicio de emisión de tarjetas criptográficas personalizadas, que permitan proteger la información que albergan con suficientes condiciones de seguridad y sean dispositivos seguros de creación de firma a los efectos de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Los soportes criptográficos se facilitarán con las utilidades software necesarias para conseguir una integración con los navegadores más utilizados y con la impresión del diseño definido por ICM, tanto en el anverso como el reverso, y los datos identificativos del usuario. El diseño de la tarjeta podrá ser modificado por ICM tantas veces considere oportuno.

Las tarjetas criptográficas, deberán tener las siguientes características:

- Acorde a los estándares ISO 7810 y ISO 7816.
- Chip inteligente con módulo criptográfico de última generación.
- Banda magnética de alta coercitividad.
- Código de acceso (PIN) a los certificados de la tarjeta. Código de desbloqueo en caso de introducir erróneamente el PIN un número determinado de veces y que la tarjeta quede bloqueada.

El adjudicatario deberá tener claramente definidos y documentados los procedimientos para la emisión de soportes criptográficos y documentación detallada y actualizada de las características técnicas de los soportes.

Adicionalmente, el adjudicatario podrá proponer a ICM la opción de emitir certificados en otros dispositivos criptográficos hardware (token, llave USB, etc) que sean dispositivos seguros de creación de firma a los efectos de la Ley 59/2003, de Firma Electrónica.

4.4 Servicio de consulta de validez de los certificados.

Se facilitarán dos tipos de servicio de consulta de validez de certificados:

- Servicio de consulta de validez de los certificados en línea a través de Internet (Online Certificate Status Protocol, **OCSP**) donde conste las circunstancias de extinción o suspensión de su vigencia.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **100031128665707605074**

- Servicio de consulta de validez a través de **listas de certificados revocados** (Certificate Revocation List, **CRL**), donde se indique los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.

El adjudicatario de los servicios recogidos en este pliego estará obligado a extender este servicio de validación asociado a los certificados emitidos durante la ejecución de este contrato, hasta finalizar su fecha de validez.

4.5 Servicio de renovación de certificados en tarjeta criptográfica por el usuario.

El servicio permitirá, en solicitudes de renovación de certificados electrónicos hardware emitidos por el prestador de estos servicios, la descarga directa online del certificado hardware por el usuario final en la tarjeta criptográfica que disponga al efecto, sustituyendo así al operador de la oficina de registro correspondiente.

El servicio asegurará que el proceso de descarga y la posterior utilización del certificado mantiene las condiciones de seguridad requeridas para este tipo de certificados hardware.

Igualmente, el servicio deberá asegurar la correcta descarga del certificado en todas las tarjetas criptográficas homologadas por ICM para este servicio.

4.6 Servicio de sellado de tiempo o de fechado digital.

Permitirá la acreditación de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos a través de una autoridad de sellado de tiempo (Time Stamping Authority -**TSA**), de tal modo que permita probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces.

Los servicios proporcionados por el TSA utilizarán como fuente fiable de tiempo el servidor NTP del Real Observatorio de la Armada, que establece el tiempo de referencia en España y cumplirá con los requisitos recogidos en la IETF RFC 3628 Policy Requirements for Time-Stamping Authorities.

La plataforma estará dimensionada de forma escalable para poder gestionar las peticiones por segundo necesarias para atender los requerimientos de la Comunidad de Madrid.

El método de comunicación entre la Comunidad de Madrid y el servicio de sellado de tiempo se realizará mediante servicios web con un sistema de autenticación basado en certificados.

La desviación máxima de los tokens de sellado será de 500ms.

El servicio de sellado de tiempo incluirá todos los elementos necesarios para su utilización, como certificados electrónicos de identificación de cliente, u otros elementos al efecto.

4.7 Servicio de información y seguimiento de certificados emitidos.

El servicio pondrá a disposición de la Comunidad de Madrid los sistemas y medios adecuados para poder consultar, de manera online y en cualquier momento, la cantidad de certificados emitidos (por fecha y tipología



de certificado) así como estadísticas de uso de los servicios contratados, y específicamente los de sellado de tiempo.

Adicionalmente a lo indicado, el adjudicatario del servicio emitirá informes mensuales detallados de la actividad realizada y de todos los tipos de certificados emitidos.

4.8 Servicio de registro de usuarios.

Para la emisión de certificados, se constituirán Oficinas de Registro que realizarán las siguientes actividades:

- Identificación de los solicitantes de los certificados, comprobación de su personalidad y constatación de su voluntad.
- Incorporación de los datos del empleado público necesarios para la emisión del certificado.
- Emisión, renovación, revocación y suspensión de los certificados, y archivo de la documentación asociada.

Existirán tres tipos de Oficinas de Registro:

- **Oficinas de registro para la emisión de certificados de empleado público**, constituidas por personal bajo el ámbito organizativo del sector público.
- **Oficinas de registro para la emisión de certificados de ciudadano**, constituidas según lo dispuesto en la Resolución de 14 de julio de 2014, del Director General de Calidad de los Servicios y Atención al Ciudadano, por la que se hace pública la relación de Oficinas de Registro de la Comunidad de Madrid, e integradas por personal de la Comunidad de Madrid.
- **Oficina de registro móvil** integrada por, al menos, dos registradores que el adjudicatario pondrá a disposición del servicio, con posibilidad de desplazarse a los centros de trabajo de los empleados públicos, para el apoyo a las Oficinas anteriores desplegadas en centros del ámbito de la Administración General de la Comunidad de Madrid e ICM, y para la emisión de certificados de sede electrónica, sello para actuación automatizada y persona jurídica. La oficina de registro móvil estará operativa desde las 9:00 hasta las 18:00 horas, de lunes a viernes, excluyendo los días inhábiles. ICM podrá solicitar la ampliación del número de registradores para atención de despliegues específicos, según las condiciones económicas recogidas en el apartado 13.2 *Servicios de coste variable*, de este pliego.

El adjudicatario proporcionará a todas las oficinas y puestos de registro los medios técnicos necesarios para expedir certificados software o hardware en soporte criptográfico, que incluirán una aplicación informática de registro y documentación asociada a la instalación y manejo de la misma, los procedimientos y normas sobre el registro, así como la formación adecuada de las personas encargadas de las oficinas de registro.

Los licitadores deberán presentar en su respuesta técnica un **Plan de Adaptación y Migración** de este servicio de registro de usuarios, de forma que se asegure la correcta continuidad del servicio de emisión,



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1000031128665707605074**

renovación, revocación y suspensión de certificados electrónicos. Este plan deberá contemplar los siguientes requisitos mínimos:

- **Oficinas de registro para la emisión de certificados de ciudadano:** migración del 50% de todas las oficinas de registro en el plazo máximo de un (1) mes desde la fecha de inicio de prestación del servicio. El 50% restante se migrará en el plazo máximo de tres (3) meses desde la fecha de inicio de prestación del servicio. Durante este periodo de migración, el adjudicatario reforzará los recursos de la oficina de registro móvil para facilitar un servicio mínimo de emisión de este tipo de certificados, en al menos dos registradores adicionales. Se valorará el incremento de este número durante la fase de migración.
- **Oficinas de registro para la emisión de certificados de empleado público, integradas por personal de ICM y Comunidad de Madrid:** migración del 80% de todos los puestos de registro en el plazo máximo de dos (2) meses desde la fecha de inicio de prestación del servicio. El 20% restante se migrará en el plazo máximo de tres (3) meses desde la fecha de inicio de prestación del servicio. Al igual que en el caso anterior, el adjudicatario presentará una propuesta de refuerzo de la oficina de registrado móvil, que asegure la continuidad en la emisión de este tipo de certificados, en al menos 2 registradores adicionales. Se valorará el incremento de este número durante la fase de migración.
- **Oficinas de registro móvil:** disponible en su totalidad desde la fecha de inicio de prestación del servicio. El plan detallará la variación de estos recursos en base al calendario global de migración.

A título orientativo, a continuación se facilita el volumen de oficinas y personal formado en actividades de registro a la fecha de elaboración de este documento. La ubicación concreta de cada oficina y puesto/s de registro se facilitará en la fase de puesta en marcha del servicio.

Oficinas de Registro y Registradores	Unidades
Oficinas de Registro para emisión de certificados de CIUDADANO	27
Registradores para emisión y renovación de certificados de CIUDADANO	63
Registradores para emisión y renovación de certificados de EMPLEADO PÚBLICO	149
Registradores para emisión y renovación de certificados de CIUDADANO y EMPLEADO PÚBLICO	73

Además, se facilitará un Plan de Formación para el personal de registro, alineado con el plan de migración de oficinas, que deberá como mínimo contener:

- Calendario detallado de acciones formativas necesarias.
- Documentación soporte detallada necesaria para la prestación del servicio.
- Manuales de uso de las aplicaciones y herramientas puestas a disposición.



4.9 Servicio de atención y soporte a registradores.

Este servicio será prestado por personal del adjudicatario, con experiencia y formación adecuada en la materia objeto del contrato, durante todo el plazo de ejecución del contrato, incluido el período de implantación del resto de los servicios recogidos en la presente cláusula, y posteriormente, durante el plazo de garantía del contrato.

Este servicio se prestará a los registradores, en días hábiles, desde las 9:00 hasta las 18:00 horas, de lunes a viernes.

El servicio ofrecerá la atención de incidencias relacionadas con el servicio prestado por los registradores desde las Oficinas de Registro, e incluirá la impartición de formación específica continua para cada uno de los diferentes perfiles de registradores al servicio de la Comunidad de Madrid, que les permita conocer y aplicar los procedimientos de registro de los diferentes tipos de certificados.

Se facilitarán informes mensuales de la actividad de este servicio, con detalle de número, tipología de incidencias y registrador que generó la incidencia, que permitan evaluar posibles puntos de mejora o refuerzo de la formación del personal de registro.

4.10 Servicios bajo demanda.

Se contemplarán en este epígrafe aquellos trabajos específicos de evolución o implementación de nuevas funcionalidades de las plataformas de emisión de certificados o de los sistemas de gestión e información del adjudicatario, y, en general, nuevos servicios relacionados con el objeto del contrato, que, a petición de ICM puedan requerirse para su implementación y/o adaptación a las necesidades específicas de la Comunidad de Madrid.

Los servicios bajo demanda, se configurarán en forma de **encargos planificables**. Para cada encargo planificable, previamente a su ejecución, el adjudicatario deberá presentar a ICM una planificación de los trabajos a realizar junto con la valoración del esfuerzo en horas. Una vez aceptada tanto la valoración como la planificación por parte de los órganos de seguimiento del contrato, podrá dar comienzo la ejecución de los trabajos asociados al encargo planificable.

En todo caso el **proceso de aceptación de los encargos planificables** contemplará:

- Adecuación de la documentación requerida.
- Cobertura de los requisitos funcionales y no funcionales.
- Idoneidad de la solución propuesta.

Todo ello condicionará la aceptación o rechazo del encargo.

La valoración económica se establecerá en base a la definición de nº de horas necesarias para la ejecución del encargo planificable correspondiente, cuyo coste hora/hombre es el recogido al efecto en el apartado 13.2 *Servicios de Coste Variable*.



CLÁUSULA 5.- FASES DE EJECUCIÓN DEL SERVICIO

La ejecución del contrato estará dividida en las siguientes fases:

5.1 Fase de Puesta en Marcha del Servicio

La fase de puesta en marcha del servicio tendrá una duración de UN MES.

En esta fase, de convivencia entre el adjudicatario del nuevo contrato y el adjudicatario del contrato vigente, se realizarán, consensuadas con ICM, las siguientes actividades orientadas a la correcta planificación y puesta en marcha de los servicios:

- Aprobación de los procedimientos operativos de gestión de los distintos certificados objeto del contrato, y documentación administrativa asociada.
- Aprobación de los procedimientos administrativos formales para la constitución de las oficinas de registro e inicio de la tramitación.
- Actualización del número de oficinas y puestos de registro constituidas al inicio de la ejecución del contrato, y aprobación del Plan de Adaptación y Migración del servicio de registro de usuarios y de formación a registradores, propuesto en la fase de licitación.
- Actualización y aprobación del calendario propuesto de formación del personal que actuará como registrador en las oficinas de registro.
- Entrega de la documentación técnica soporte de la actividad en forma de manuales de uso, ayuda on-line o similar, del sistema de gestión a utilizar para la emisión de certificados y de los procesos de descarga e instalación posterior de los certificados en el navegador o dispositivo criptográfico elegido.
- Las librerías, módulos criptográficos, clientes software, etc., a instalar en los equipos designados por ICM, necesarios para la emisión de los certificados.
- Un juego completo de certificados de prueba, para uso por parte del personal de ICM.
- La propuesta y ejecución de las pruebas técnicas necesarias para la instalación del servicio de sellado de tiempo en la infraestructura de certificación y firma de ICM.

En esta fase ICM facilitará, para el servicio de emisión de soportes criptográficos, la información de diseño de la tarjeta que deberá aplicarse.

5.2 Fase de Pleno Servicio

La Fase de Pleno Servicio comenzará el 1 de junio de 2015 y tendrá una duración de **36 meses**, salvo en caso de prórroga del contrato.

El adjudicatario deberá proporcionar todos los servicios en los términos y condiciones establecidos en este pliego, a excepción del Servicio de Registro de Usuarios en su componente de constitución de oficinas de registro y puestos de registro, que se ajustará al plan de adaptación y migración del servicio y calendario de formación de registradores, aprobado por ambas partes en la fase de puesta en marcha del servicio.



5.3 Transición de Salida

El adjudicatario deberá realizar todas las labores necesarias para garantizar la transferencia del servicio. Para ello, deberá presentar a ICM, para su aprobación, un Plan de Transferencia, en el que, con todo detalle, se expongan los contenidos técnicos y funcionales de las actividades llevadas a cabo a lo largo del servicio. Dicho Plan de Transferencia será entregado por el adjudicatario **tres meses** antes de la finalización del contrato para su validación por ICM.

Un mes antes de la finalización del contrato se pondrá en marcha el plan aprobado para realizar la transferencia de servicio. Esta fase de transición de salida del adjudicatario saliente se corresponderá con la fase de puesta en marcha del adjudicatario entrante. El adjudicatario se compromete a garantizar la completa y correcta operatividad del servicio prestado, al amparo del expediente, durante el periodo de transición de salida requerido a la finalización del contrato, que permita el cambio de dicho adjudicatario del servicio.

CLÁUSULA 6.- ACUERDOS DE NIVEL DE SERVICIO

6.1 Niveles de servicio.

6.1.1 Prestación del servicio.

El servicio de registro de usuario deberá estar en funcionamiento en los plazos recogidos en el apartado 4.8 *Servicio de registro de usuario*.

Los servicios de tramitación, emisión y entrega de certificados no emitidos por personal de la Comunidad de Madrid como son los certificados de sede, sello electrónico, componente y persona jurídica, que no incluyan el suministro de un soporte físico se realizará en un plazo máximo de **cinco (5) días hábiles**. En caso de requerir emisión en soporte criptográfico, se realizará en un plazo máximo de **siete (7) días hábiles**.

En el caso de los soportes criptográficos, una vez que ICM comunique al prestador del servicio la información necesaria para la personalización de los soportes, éste dispondrá de un plazo máximo de **dos (2) semanas** para la emisión física de los soportes y su puesta a disposición de ICM.

6.1.2 Resolución de incidencias y disponibilidad del servicio.

Se considera incidencia cualquier situación que suponga la interrupción, degradación o falta de información o de documentación suficiente, de cualquiera de los servicios requeridos en el presente pliego.

El plazo de resolución de una incidencia es el período comprendido entre el momento de comunicación por parte de ICM de una incidencia, y la resolución completa de la misma por parte del adjudicatario.

Las incidencias se clasificarán en tres tipos, en función de su gravedad:

- Se asignará un *nivel alto* a la incidencia que suponga la interrupción de un servicio.
- Se asignará un *nivel medio* a la incidencia que suponga la degradación de un servicio.



- Se asignará un *nivel bajo* a la incidencia que suponga falta de atención o cumplimiento a requerimientos de información y clarificación sobre aspectos técnicos relacionados con los servicios.

El nivel de gravedad será asignado por ICM en el momento de abrir una incidencia. El adjudicatario presentará en la fase de licitación los mecanismos, interlocutores, puntos de contacto, y procedimientos establecidos para la notificación y tratamiento de las incidencias relacionadas con el servicio demandado.

Las incidencias deberán ser resueltas en los siguientes plazos máximos:

- Las incidencias con nivel alto, en **4 horas**.
- Las incidencias con nivel medio, en **8 horas**.
- Las incidencias con nivel bajo, en **2 días hábiles**.

Se informará a ICM en todo momento y de manera detallada de cualquier acción a tomar para la resolución de una incidencia.

Una incidencia se cerrará cuando ICM haya aceptado dicho cierre, lo que normalmente se producirá cuando el servicio se haya restablecido y estabilizado, se hayan eliminado o corregido las causas que originaban los problemas en el servicio y se haya informado a ICM de dichas causas y confirmado que estas se han eliminado.

El adjudicatario deberá además, en caso de necesidad, prestar el soporte técnico necesario, in situ o de forma remota, al operador de ICM ante una tarea preventiva o correctiva.

En cuanto a los requisitos de disponibilidad aplicables a los servicios de sellado de tiempo y de consulta de validez de los certificados, deberán estar operativos durante las **24 horas del día**, los **365 días del año**.

Los servicios de información y seguimiento de certificados emitidos y estadísticas de uso de los servicios, y de atención y soporte a registradores, estarán operativos desde las 9:00 hasta las 18:00 horas, de lunes a viernes, excluyendo los días inhábiles.

6.2 Cálculo de penalizaciones

El incumplimiento de los niveles de servicio establecidos queda sujeto a las siguientes penalizaciones. En caso de que la cuantía acumulada de las penalizaciones supere el 10% del importe de adjudicación, ICM quedará facultada para instar la resolución del contrato.

6.2.1 Prestación del servicio.

En el caso de los servicios de emisión, renovación, revocación y suspensión de certificados de empleado público y ciudadano a través de oficinas de registro en la Comunidad de Madrid, por cada día de retraso en la puesta en funcionamiento del servicio de registro, se aplicará una penalización de **500 €/día**.

En el caso de los servicios de emisión, renovación, revocación y suspensión de certificados de componente, de emisión de soportes criptográficos, de consulta de validez de los certificados, de renovación de certificados en



tarjeta, de sellado de tiempo, y de información y seguimiento de certificados emitidos, por cada día de retraso en la puesta en funcionamiento de los servicios, se aplicará una penalización por importe de **300 €/día**.

En el caso de los servicios de emisión, renovación, revocación y suspensión de certificados sede, sello electrónico, componente y persona jurídica, con o sin soporte criptográfico, por cada día de retraso en la entrega de los elementos, se aplicará una penalización de **400 €/día**.

6.2.2 Resolución de incidencias y disponibilidad del servicio.

En el caso de incidencias de nivel alto en los servicios objeto del contrato, se aplicará una penalización por importe de **500 €/día** por cada día de retraso en su resolución.

En el caso de incidencias de nivel medio y bajo, por cada día de retraso en la resolución se aplicará una penalización por importe de **400 €/día y 300 €/día**, respectivamente.

En el caso de indisponibilidad en la prestación de alguno de los servicios de consulta de validez de los certificados, de sellado de tiempo, y de verificación de firma, se aplicará una penalización por importe de **100 € por cada hora de indisponibilidad**.

En el caso de indisponibilidad en la prestación de alguno de los servicios de información y seguimiento de certificados emitidos, y de atención y soporte a registradores, se aplicará una penalización por importe de **50 € por cada hora de indisponibilidad**.

La cuantía de las penalizaciones que se descuenten en una factura no podrá superar el 30 % del importe de la misma, sin perjuicio de la aplicación del resto del importe no descontado en la/s siguiente/s factura/s.

CLÁUSULA 7.- EQUIPO ADSCRITO A LA PRESTACIÓN DEL SERVICIO

El contratista responderá siempre de la adecuación del personal asignado a la prestación de los servicios que constituyen el objeto del contrato.

Para la prestación de los servicios objeto del contrato, el adjudicatario designará al menos:

- 1 Responsable del Servicio ante ICM.
- Equipo de registradores de la Oficina de Registro Móvil.
- 1 Jefe de Proyecto para soporte a proyectos.

En el plazo indicado en la cláusula 14 del Pliego de Cláusulas Jurídicas, el licitador propuesto como adjudicatario deberá aportar **Curriculum Vitae del Responsable del Servicio, del Jefe de Proyecto y de los miembros del equipo de Registradores de la Oficina de Registro Móvil**, según el modelo incluido en el **Anexo "Modelo de Currículum" al presente Pliego**, que deberán aportar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando su cualificación profesional (con detalle de categoría, titulación, formación y actividad profesional), así como toda aquella documentación que ICM estime necesaria para la acreditación de los datos contenidos en dichos Currículos.





En el caso de que se presten servicios en las instalaciones de ICM, el personal de la empresa contratista que ejecute por cuenta de ésta trabajos directamente relacionados con el objeto del presente contrato, **utilizarán los medios de producción físicos y lógicos** de que hayan sido provistos por la propia empresa contratista, salvo que por razones operativas asociadas a la naturaleza del servicio a prestar, ICM proporcione medios, en todo caso con carácter transitorio, a la empresa contratista, ya que se utilizarán únicamente durante la ejecución del contrato y además su uso estará limitado exclusivamente al desarrollo de los trabajos que constituyen el objeto del mismo.

7.1 Responsable del Servicio ante ICM

El adjudicatario designará a un **Responsable del Servicio ante ICM**. Este Responsable se encontrará en permanente contacto con el personal que la Dirección de ICM designe.

En particular, este responsable, realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y la formación necesaria que el adjudicatario suministrará al equipo humano que realice los trabajos objeto del presente contrato, en todas aquellas materias que sean necesarias para el perfecto desempeño de dichos trabajos.
- Supervisar y controlar el trabajo realizado y las actividades realizadas e informar a ICM de las posibles incidencias y seguimiento o desviaciones de plazos.
- Ejercer el mando y el poder organizativo sobre el equipo humano del adjudicatario destinado a atender los servicios objeto del presente contrato, que estará siempre bajo la disciplina laboral y el poder de dirección del adjudicatario, independientemente de que, para el mejor cumplimiento del servicio, en determinados momentos, pueda el adjudicatario destacar su personal en cualquier centro de trabajo, oficinas o ubicaciones de la Comunidad de Madrid.
- Gestionar las incidencias que se produzcan y que sean emitidas por los integrantes del equipo de trabajo adscrito a la ejecución de este contrato.

El incumplimiento de las obligaciones precitadas, parcial o totalmente, facultará a esta Agencia para instar a la resolución del contrato.

7.2 Equipo de registradores de la Oficina de registro móvil

El adjudicatario deberá poner a disposición del servicio un equipo de registradores de la Oficina de Registro Móvil, integrado, al menos, por dos personas, y los medios técnicos necesarios para dar el servicio de emisión, revocación, suspensión y registro de certificados.



7.3 Jefe de Proyecto para soporte a proyectos

El adjudicatario del contrato pondrá a disposición de ICM un Jefe de Proyecto que facilite la interlocución y coordinación técnica y organizativa con el adjudicatario para los proyectos que ICM ejecute dentro del ámbito de los servicios que constituyen el objeto del contrato.

CLÁUSULA 8.- MODELO DE SEGUIMIENTO DE LA EJECUCIÓN DEL CONTRATO

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de ICM, con objeto de garantizar la correcta ejecución de los mismos.

De cara a alcanzar estos objetivos se define una estructura de seguimiento de **dos niveles**:

- Un **nivel estratégico** orientado a la evolución del contrato y la mejora de los servicios, que se encargará de velar porque la estrategia y objetivos de la contratación de certificados y servicios estén alineados con los de ICM, y de controlar y garantizar que todas las decisiones y operaciones se ajustan a dicha estrategia.
- Un **nivel operativo** ligado a la ejecución concreta de los certificados y servicios que se encargará de transformar las decisiones estratégicas en planes de acción y de dirigir y controlar los esfuerzos necesarios para su ejecución. En este nivel el adjudicatario se responsabiliza de la gestión, ejecución, supervisión técnica y control diario de los certificados y servicios.

Atendiendo a la estructura señalada se establecerán dos Comités diferenciados para el control y la toma de decisiones:

- Comité de Seguimiento del Contrato (estratégico)
- Comité Operativo (operativo)

8.1 Comité de seguimiento del contrato

Estará compuesto por los siguientes miembros:

Por parte de **ICM**:

- El Subdirector General de Tecnología, a petición propia.
- El Director competente en materia de Ingeniería.
- El Director competente en materia de Administración Electrónica.
- El Director competente en materia de Seguridad Corporativa.
- Opcionalmente, y por indicación del responsable del contrato el/los Director/es competentes en materia de Producción y Servicios a Cliente o cualquier otro de ICM requerido.

Estos miembros podrán ser sustituidos por persona perteneciente a su Dirección, designada por ellos mismos con antelación suficiente.



Por parte de la **empresa adjudicataria**:

- El Responsable del Servicio ante ICM.

No obstante lo anterior, se podrá requerir la presencia de otros miembros distintos a los señalados que se estimen oportunos para la correcta realización de las sesiones de los mismos.

El Comité de Seguimiento del Contrato se desarrollará en reuniones con **periodicidad trimestral**, y tendrá entre otras, las siguientes **funciones**:

1. Monitorizar el avance global de los certificados y servicios.
2. Aprobar los cambios propuestos en el seno de los Comités Operativos que afectan de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o que, por su impacto o importancia estratégica, requieran la aprobación del Comité.
3. Controlar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo.
4. Acordar la adopción de propuestas de mejora y medidas correctoras o preventivas que deba desarrollar e implantar el adjudicatario, previa autorización de ICM, en caso de incumplimiento de los ANS o derivadas de planes de mejora.
5. Revisar los niveles de servicio inicialmente requeridos, en base a la mejora continua del mismo.
6. Definir y aprobar nuevos acuerdos de niveles de servicio y régimen de penalizaciones, no mencionados en este Pliego y considerados imprescindibles para la correcta prestación del servicio.
7. Determinar el grado de incumplimiento de ANS con el objeto de aplicar las correspondientes penalizaciones que se establecen en el presente pliego de cláusulas técnicas.
8. Revisar y aprobar el borrador de factura y resolver cualquier incidencia o problema relacionado con los certificados y servicios a facturar en el periodo objeto de revisión.
9. Cualquier otro asunto que el propio Comité considere de interés.

La Agencia podrá convocar reuniones extraordinarias por la existencia de circunstancias que lo hagan necesario.

Los acuerdos adoptados en el seno del Comité de Seguimiento deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas, y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

8.2 Comité operativo

Estará formado como mínimo por los siguientes miembros:

Por parte de **ICM**:



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **100003112866570605074**



- Los Jefes de las áreas responsables del seguimiento de los certificados y servicios.
- Los responsables del seguimiento de los certificados y servicios.

Estos miembros podrán ser sustituidos por personal perteneciente a su Dirección, designada por ellos mismos con antelación suficiente.

Por parte de la **empresa adjudicataria**:

- Responsable del Servicio ante ICM.
- Jefe de Proyecto.

No obstante lo anterior, se podrá requerir la presencia de otros miembros distintos a los señalados que se estimen oportunos para la correcta realización de las sesiones de los mismos.

El Comité Operativo se reunirá con **periodicidad mensual** y tendrá, entre otras, las siguientes **funciones**:

1. Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de riesgos.
2. Garantizar que el personal asignado por el contratista para la ejecución de los servicios está disponible, y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.
3. Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo.
4. Analizar y validar si procede las propuestas de mejora del servicio efectuadas por el adjudicatario. En caso de que las propuestas afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o tengan impacto o importancia estratégica, serán elevadas al Comité de Seguimiento del Contrato.
5. Revisar el estado y evolución de los Planes de mejora acordados y cumplimiento de los compromisos aprobados.
6. Cualquier otro asunto que el propio Comité considere de interés.

Los acuerdos adoptados en el seno del Comité deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas, y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

8.3 Informes de Seguimiento del Servicio

El adjudicatario proporcionará a ICM informes de gestión, en soporte electrónico compatible con Microsoft Office, con periodicidad trimestral, y con al menos 48 horas de antelación a las reuniones del Comité de Seguimiento, sin perjuicio de la potestad de ICM para exigir otros informes cuando así lo demande.



Asimismo, se emitirá un informe por el adjudicatario antes de la última semana de vigencia del contrato.

8.4 Modelo de Gestión de Atención de Incidencias y Soporte técnico

Durante todo el periodo de vigencia del contrato y para todos los servicios solicitados, el adjudicatario establecerá un modelo de Atención y Asistencia a Incidencias y Soporte técnico en los siguientes términos:

- Soporte **telefónico** por personal técnico cualificado. El horario será de 9:00 a 18:00 horas, de lunes a viernes, en días hábiles.
- Soporte a través de un **portal web** para la gestión de las incidencias y consultas de soporte técnico. Este portal deberá estar disponible 24 horas al día durante los 7 días de la semana.
- Ambos soportes (telefónico y portal web) atenderán:
 - o Gestión de Incidencias. Apertura, documentación asociada, seguimiento, estado, resolución. A cada incidencia se le asignará un número para facilitar su identificación y seguimiento.
 - o Consultas planteadas respecto a la operativa y funcionamiento de los servicios ofertados. Soporte técnico.
- En caso de considerarlo necesario y ante incidencias que supongan una caída de los servicios que presta ICM, se podrá requerir un soporte in situ (presencia física de un técnico del adjudicatario) para agilizar la resolución y proporcionar el soporte necesario a las áreas técnicas correspondientes.
- El Modelo de Gestión de Atención y Soporte de Incidencias tendrá un único interlocutor ante ICM, representado en la figura del Responsable del Servicio ante ICM.
- El responsable del servicio ante ICM enviará un informe de las incidencias reportadas, estado y actuaciones realizadas sobre ellas, con al menos 48 horas de antelación a las reuniones del Comité Operativo.

La periodicidad de dichos informes será mensual, pudiendo ser modificada a requerimiento de ICM cuando las circunstancias lo aconsejen.

CLÁUSULA 9.- PLAZO DE GARANTÍA

Se establece un plazo de garantía del contrato de **DOCE (12) MESES**, cuyo cómputo se iniciará desde la fecha de recepción o conformidad de los trabajos.

Hasta que no tenga lugar la finalización del periodo de garantía, el contratista responderá de la correcta realización de los trabajos ejecutados, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de ICM los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los certificados o servicios efectuados.



CLÁUSULA 10.- GESTIÓN DE LA SEGURIDAD

Las medidas de seguridad de los servicios prestados por el adjudicatario deberán adecuarse a las políticas y normativa en materia de seguridad de ICM en cada momento, considerando que estas políticas irán evolucionando y mejorando con carácter continuo.

La Administración de la Comunidad de Madrid, a través de la Dirección General de Calidad de los Servicios y Atención al Ciudadano o de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid (ICM), podrá verificar en cualquier momento, por sí o por medio de agentes autorizados, que la expedición de los certificados o cualquier otro aspecto de los sistemas de firma electrónica que operen en la Comunidad se estén realizando conforme a las condiciones establecidas en el presente pliego y en la normativa vigente, y en concreto en el Decreto 94/2006, de 8 noviembre de Utilización de la firma electrónica en las relaciones con la Administración de la Comunidad de Madrid por medios electrónicos, informáticos y telemáticos.

El adjudicatario debe analizar el servicio prestado y adoptar las medidas oportunas para su corrección en caso de detectar patrones sospechosos, en materia de seguridad, que pudieran suponer mal uso, detección de anomalías, intrusiones y otros.

Asimismo, el adjudicatario alertará a los equipos responsables del servicio de ICM, en caso de detectar intrusión o presencia interna en los sistemas o equipamientos del servicio para ICM de virus, troyanos o cualquier anomalía que pudiera afectar a la seguridad de la información.

El adjudicatario tiene expresamente prohibido hacer público cualquier detalle o información relativa a la estructura, ubicación, configuración y uso de las infraestructuras y servicios que utiliza o presta en o para ICM. Asimismo, no informará de la situación presente o futura de cualquier servicio o incidencia, a ninguna persona que no se encuentre autorizada e identificada como interlocutor válido por la Dirección responsable del contrato por parte de ICM.

En este mismo sentido, tiene la obligación de no comunicar el usuario y/o contraseña de acceso a servicios, sistemas o equipamientos, a ninguna persona u organización que no esté identificada y autorizada por la Dirección responsable del contrato por parte de ICM como interlocutor válido para el manejo de este tipo de información.

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención a la observancia de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, el *Real Decreto 1720/2007, de 21 de diciembre*, por el que se aprueba el Reglamento de desarrollo de la anterior, la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* y el *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*.

Respecto a la gestión, administración y operación de los sistemas de información y de los datos a que se tenga acceso, todo ello dentro de la realización de los trabajos objeto del presente contrato, se deberán cumplir los



requisitos de seguridad recogidos en este clausulado en todas las infraestructuras, servicios y sistemas del adjudicatario que den servicio a ICM en el desarrollo del contrato.

El adjudicatario estará obligado a la realización y al mantenimiento de los registros de evidencias del cumplimiento, durante al menos todo el periodo de ejecución del contrato, de las actividades relacionadas a continuación:

- a) Definir, implementar y mantener una política de seguridad de la información.
- b) Implementar los análisis, ingeniería y contramedidas de seguridad con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información, mediante la ejecución de los controles que den respuesta a los requisitos especificados en este clausulado; todo ello integrado en una gestión de análisis y gestión del riesgo.
- c) Extender lo especificado en el punto anterior a los posibles contratos o relaciones con terceros vinculados a sistemas de información, productos y servicios que estén relacionados con la prestación del servicio objeto del contrato.
- d) En la fase de diseño funcional de los desarrollos objeto del contrato se realizará un estudio previo de su naturaleza y las medidas de seguridad que requieran de conformidad con la naturaleza de la información y el servicio que soportan y los requerimientos de la distinta normativa que les aplique. Esta especificación de requisitos de seguridad se documentará conforme a lo establecido en los estándares de ICM al respecto de la materia.

Los siguientes apartados establecen las condiciones y medidas en materia de seguridad que el adjudicatario deberá implantar y mantener para la prestación del servicio. Estas condiciones y medidas se considerarán como de obligado cumplimiento y con carácter de mínimos, teniendo en cuenta que el adjudicatario podrá implantar adicionalmente otros que considere adecuados o necesarios a lo largo de la ejecución del contrato. En todo caso, se estará a lo dispuesto en los estándares de seguridad de ICM. Asimismo, ICM podrá modificar esta relación de requisitos mínimos en cualquier momento, comunicando dicha variación al adjudicatario, quién estará obligado a adecuar sus sistemas a la modificación.

10.1 Documentación de seguridad

El adjudicatario deberá entregar los siguientes documentos, que deberán estar permanentemente actualizados y a disposición de ICM en cualquier momento de la ejecución del contrato:

- a) Un documento denominado **Política de Seguridad**, que estará basada en la Política de Seguridad Corporativa de ICM, que consistirá en un documento de alto nivel, que defina lo que significa la "Seguridad de la Información" en la organización, y aplicable al servicio prestado. El documento deberá estar accesible por todos los miembros de la organización que intervengan en la prestación del servicio y redactado de forma sencilla, precisa y comprensible.
- b) Un documento denominado **Documento de Seguridad**, coherente con los documentos de seguridad que exigen los *Reales Decretos 1720/2007*, y *3/2010* respectivamente, en lo que corresponda a cada uno,



donde se encuentre la normativa de seguridad que recoja todas las medidas de seguridad propuestas, la forma de su cumplimiento y las responsabilidades asociadas, con indicación expresa de la identidad del *Responsable de Seguridad del Servicio*. Estas medidas de seguridad incluirán al menos las que se relacionan a continuación para cada uno de los ámbitos normativos.

10.2 Usuarios de sistemas de información

Los usuarios de los sistemas de información relacionados con el objeto del servicio deberán estar identificados y autorizados por el adjudicatario y quedar así reflejado en el *Documento de Seguridad*, previamente a efectuar cualquier uso de los sistemas mediante, el correspondiente procedimiento que incluya los procesos de identificación, autenticación y autorización.

En el *Documento de Seguridad* se incluirá además la correspondencia y relación de los perfiles y las funciones asociadas al servicio prestado para ICM, así como las personas asociadas a dichos perfiles que pudieran tener acceso a información de la Comunidad de Madrid, y el tipo de información a la que pudieran tener acceso, ya sea datos de carácter personal, de administración electrónica u otro tipo.

Se registrará además en el *Documento de Seguridad*, si se diera la circunstancia, la relación de usuarios con privilegios de administración de los sistemas de información de ICM (asociados a posibles tareas habituales o puntuales de mantenimiento, explotación de sistemas o cualquier otra que pudiera implicar el acceso a datos del entorno de producción de los sistemas de información de la Comunidad de Madrid).

En el caso de utilizar sistemas de información de la Comunidad de Madrid, deberán acreditarse previamente de acuerdo con la política de gestión de identidades corporativa de ICM.

Se deberá acreditar el conocimiento y compromiso de la cláusula de seguridad de este pliego por parte de todos los usuarios, quedando registrado en el *Documento de Seguridad*, así como la renuncia expresa de los derechos de propiedad intelectual que les pudiera corresponder. Las obligaciones subsistirán aun después de finalizar la relación contractual.

El contratista se compromete a formar e informar a su personal en las obligaciones que de estas cláusulas y la normativa que se menciona dimanar, para lo cual programará las acciones formativas necesarias.

Las relaciones de usuarios mencionadas deberán estar permanentemente actualizadas durante la prestación del servicio.

10.3 Protección de datos de carácter personal.

En el caso de que el contratista, en el ejercicio de la prestación del servicio, tuviera que tratar ficheros con datos de carácter personal en el marco del objeto del presente contrato, cumplirá con la legislación vigente en materia de protección de datos de carácter personal conforme a lo dispuesto en las leyes y decretos que se relacionan a continuación:

- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD.*



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **100031128665707605074**

- *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en los términos previstos en su Disposición Transitoria Segunda).*
- *Disposiciones de desarrollo de las normas anteriores en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.*

Medidas de seguridad de carácter mínimo.

1. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el R.D. 1720/2007 respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. (Artículo 9.2. LOPD):
 - 1.1. En la fase de diseño funcional, y si del estudio previo de cada sistema de referencia procediera se propondrá la correspondiente creación e inscripción en la Agencia Española de Protección de Datos (en adelante AEPD).
 - 1.2. Los diseños, desarrollos o mantenimientos de software deberán, con carácter general, observar los **estándares** que se deriven de la **normativa de seguridad** de la información y de protección de datos de ICM, y en concreto:
 - 1.2.1. Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
 - 1.2.2. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado por la Agencia ICM. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por ICM. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
 - 1.2.3. Lo relativo a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Con una periodicidad no superior a un año se cambiarán las contraseñas asignadas a los usuarios, las cuales, mientras estén vigentes, se almacenarán de forma ininteligible.
 - 1.2.4. Solo con el consentimiento expreso y escrito de ICM, el equipo prestador del servicio objeto del contrato tendrá acceso y tratará datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.



- 1.2.5. Deberán realizarse, como mínimo semanalmente, copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- 1.2.6. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento.
- 1.2.7. Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.
- 1.2.8. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
- 1.3. Además de las medidas hasta aquí enumeradas, los tratamientos de datos de carácter personal relativos a la comisión de **infracciones** administrativas o penales, procedimientos **tributarios**, o aquéllos que contengan datos que ofrezcan una definición de las características o de la **personalidad** de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, deberán observar las siguientes medidas:
 - 1.3.1. Deberá establecerse un sistema de registro de entrada y de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada.
 - 1.3.2. Exclusivamente el personal autorizado por ICM podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
 - 1.3.3. Será necesaria la autorización de ICM para la ejecución de los procedimientos de recuperación de los datos.
- 1.4. Además de las medidas enumeradas en los anteriores apartados 2.1, 2.2 y 2.3, los tratamientos de datos de carácter personal relativos a **ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual** (salvo los tratados para verificar meras transferencias dinerarias, o los referentes exclusivamente al grado o condición de discapacidad o invalidez con motivo del cumplimiento de deberes públicos, a los que se les aplican las medidas del anterior apartado 2.2); los que contengan o se refieran a datos recabados para **finés policiales**; o aquéllos que contengan datos derivados de actos de **violencia de género**, deberán observar las siguientes medidas:



- 1.4.1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de ICM.
- 1.4.2. Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en la normativa de protección de datos personales, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.
- 1.4.3. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

El registro de los accesos deberá integrarse con el sistema de información de la Comunidad de Madrid para la gestión y explotación de la información resultante de los accesos (SGUR).
- 1.4.4. El período mínimo de conservación de los datos registrados será de dos años. El contratista se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
- 1.4.5. Cuando se transmitan datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Cesión o comunicación de datos a terceros.

2. Los datos de carácter personal o documentos objeto del tratamiento **no podrán ser comunicados a un tercero** bajo ningún concepto, sin el consentimiento del titular del dato y el conocimiento de ICM, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
3. El contratista tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con un fin distinto al que figure en el objeto del contrato, ni los **comunicará**, ni siquiera para su conservación, a otras personas.

A la finalización del contrato, según el criterio o indicación de ICM, el equipo prestador del servicio procederá a destruir o a devolver a ICM toda la información confidencial o cualquier dato de carácter



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1000031128665707605074**

personal que haya sido susceptible de ser tratado durante la prestación del servicio, independientemente de que haya sido de forma escrita, grabada o empleando cualquier otro soporte en que pudiera recogerse.

La destrucción o devolución de la información confidencial o cualquier dato de carácter personal no exonerará al equipo prestador del servicio de su obligación de tratar dicha Información Confidencial como estrictamente confidencial aún finalizada la relación convencional existente entre las mismas.

En el caso de que el contratista destine los datos a **otra finalidad, los comunique o los utilice incumpliendo** las estipulaciones del contrato, será considerado como único responsable, respondiendo de las infracciones en que hubiera incurrido personalmente.

4. De acuerdo con lo dispuesto en el *Artículo 10 apartado Tres letra c) de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas*, ICM, que **actúa en nombre y por cuenta del Responsable del Fichero o Tratamiento**, ejerce como función la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente la administración, mantenimiento y soporte de los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones de cualquier especie que se encuentren instalados en la misma.

La contratación de las funciones propias del *Encargado del Tratamiento* de datos de carácter personal, será realizada de conformidad con lo dispuesto en el *Artículo 21 del RD 1720/2007*, se limitará a los servicios que constituyen el objeto del presente contrato.

El contenido del servicio contratado estará determinado por el conjunto de derechos y obligaciones que, en virtud del presente contrato, asume el contratista como encargado del tratamiento de datos personales. Sin perjuicio de las instrucciones que, adicionalmente, pudieran establecerse por el **Encargado del Tratamiento**, el contratista queda sujeto en el tratamiento de datos personales a las instrucciones procedentes del **Responsable del Fichero**.

El contratista se obliga a cumplir las medidas de seguridad establecidas en el *Artículo 9 de la LOPD* y las previstas en el *R D 1720/2007*, en los mismos términos que el **Responsable del Tratamiento**

Derecho de información en la recogida de datos.

5. Los datos personales recogidos podrán ser incorporados y tratados en el fichero **PROVEEDORES**, cuya finalidad es la solicitud de ofertas, selección y compra de bienes y servicios requeridos tanto por ICM como por la C.M., inscrito en el Registro General de Protección de Datos de la AEPD (www.agpd.es), y no podrán ser cedidos salvo en los supuestos previstos en la Ley. El responsable del fichero es ICM, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es la calle Embajadores Nº 181, de Madrid, todo lo cual se informa en cumplimiento del Artículo 5 de la LOPD.

10.4 Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1000031128665707605074**

El adjudicatario asumirá el cumplimiento de lo establecido en el *Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 enero - ENS)* en lo referido a la adopción de medidas de seguridad de los servicios prestados. Se tendrá en cuenta la aplicación de las medidas de seguridad establecidas en el *Anexo II del ENS*, a una o varias dimensiones de seguridad y según el nivel determinado en cada caso.

El adjudicatario deberá realizar las acciones necesarias para concienciar regularmente al personal interviniente en la prestación del servicio acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

Se formará regularmente al personal interviniente en la prestación del servicio en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán las medidas de seguridad indicadas en su *Anexo II*, ya sean pertenecientes al marco organizativo, operacional o de protección.

El Documento de Seguridad reflejará, además de lo estipulado con carácter general, la relación de las medidas de seguridad y de la forma en la que se procederá al cumplimiento en materia de seguridad en los sistemas de información de administración electrónica en el transcurso del desarrollo de los trabajos.

10.5 Medidas de seguridad y compromisos del adjudicatario en el caso de acceso remoto a infraestructuras de ICM

En el caso de que el adjudicatario acceda de forma remota desde sus instalaciones a infraestructuras de la Comunidad de Madrid, será de aplicación lo especificado a continuación.

La información asociada a los accesos a infraestructuras de producción de ICM que alberguen datos o información de la Comunidad de Madrid durante el periodo de ejecución de los servicios y del periodo de garantía de los mismos deberá estar a disposición de ICM, y contemplará las acciones de realizadas por cada usuario, el motivo, la solicitud y autorización de ICM, el mecanismo utilizado, así como todos los datos referidos a los dispositivos y mecanismos utilizados.

Además, se deberán cumplir las siguientes medidas de seguridad:

- No se habilitarán ni utilizarán las funciones de las aplicaciones o sistemas operativos que permitan guardar o recordar las credenciales de acceso de forma automática.
- Las infraestructuras del adjudicatario que se utilicen para dar cumplimiento al objeto del contrato y que deban acceder a la red corporativa de la Comunidad de Madrid deberán estar aisladas lógicamente y físicamente, de forma que dichas infraestructuras se utilicen de forma exclusiva para la prestación de los servicios, debiéndose asegurar que no existen conexiones directas entre cualquier otra red distinta de la habilitada para la prestación del servicio y cualquier red de la Comunidad de Madrid a la que se acceda en virtud del contrato ya sea una red pública (ej. Internet) o privada, exceptuándose las conexiones autorizadas requeridas para la prestación del servicio.



- Entre cada red, subred o servicio de comunicaciones se implantarán cortafuegos (firewalls), que deberán estar configurados con la política del menor privilegio, bloqueando o denegando cualquier tipo de tráfico no autorizado o innecesario para la prestación del servicio. De la misma forma se permitirán únicamente los puertos, protocolos o servicios autorizados por ICM. Cualquier puerto, protocolo o servicio no especificado como autorizado se denegará por defecto.
- Los accesos a Internet se efectuarán obligatoriamente a través de proxies con sistema de identificación de su uso.
- El uso del correo electrónico deberá contar con filtro antivirus debidamente actualizado periódicamente.
- No se compartirán las cuentas de correo asignadas de forma personal, ni se podrá desviar de forma automática el correo electrónico profesional a cuentas particulares.
- El adjudicatario deberá implantar un Plan de Contingencia que ofrezca respuesta a emergencias, operaciones de respaldo y restauración y contingencias, que, al menos, garantice la correcta operación y entrega de los servicios según los niveles de servicio especificados en el apartado correspondiente.
- Se implementarán salvaguardas para detectar o minimizar la modificación o destrucción no autorizada de datos.
- Se mantendrá y ejecutará una política de respaldo automático de datos, verificación y restauración (en su caso).
- La información que deba suprimirse deberá destruirse de tal forma que sea imposible su recuperación.
- Se incluirá un sistema de protección antivirus, actualizado periódicamente y de forma automática, y que deberá utilizarse sobre cualquier fichero, soporte y software antes de que cualquiera de éstos resida o se instale en los sistemas de información. La frecuencia de actualización será como mínimo semanal.

10.6 Propiedad de los trabajos

Todos los derechos de propiedad intelectual o industrial sobre los trabajos, informes, estudios y documentos, así como los productos y subproductos elaborados por la empresa adjudicataria y el personal encargado de la ejecución del objeto de la relación contractual serán propiedad de ICM, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello la empresa contratista.

La empresa adjudicataria y su personal renuncia expresamente a cualquier derecho que sobre los trabajos realizados pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de ICM.

Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo del contrato resultante de la adjudicación resultante de la presente licitación corresponden únicamente a ICM.

10.7 Sigilo y Confidencialidad de la información tratada

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

Esta obligación no se limita al tiempo de ejecución del correspondiente contrato al que está asociado el proyecto indicado, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier Información, fuese cual fuere su naturaleza (bien técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por ICM o la Comunidad de Madrid o cualquier tercero que tenga relaciones contractuales con la misma, en relación con el objeto del presente pliego, será considerada como "Información Confidencial", incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

La empresa adjudicataria y el personal encargado de la realización de las tareas (en adelante el Equipo del Proyecto) se obligan a:

- Guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el Equipo del Proyecto;
- Utilizar o transmitir la Información Confidencial exclusivamente para los fines del objeto del contrato;
- No realizar copia de la Información Confidencial sin el previo consentimiento escrito de ICM, excepto aquellas copias que sean necesitadas por el Equipo del Proyecto para su estudio interno;
- Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento;
- No facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito de ICM, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los del presente documento.
- Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del contrato o su contenido, deberá ser previamente aprobada por escrito por ICM.
- El Equipo del Proyecto procederá a destruir o a devolver a ICM toda la Información Confidencial a la finalización del objeto del contrato referido, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida.
- La empresa contratista formará e informará de estas obligaciones al personal que participe en el desarrollo del contrato, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.



10.8 Restricciones generales

En el marco de la ejecución del contrato, y respecto a los sistemas de información que le dan soporte, las siguientes actividades están específicamente prohibidas:

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remoto a usuarios no autorizados.
- Inutilizar o suprimir cualquier elemento de seguridad o protección o la información que generen.

10.9 Auditoría de la seguridad y trazabilidad de los servicios

El adjudicatario adquirirá el compromiso de ser auditado por personal autorizado por ICM en cualquier momento en el desarrollo de los trabajos, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

Asimismo, y en el marco de la ejecución de los trabajos, y con el fin de garantizar la seguridad de la información manejada, ICM se reserva la capacidad de monitorizar la actividad de los sistemas, por lo que se informará a los usuarios de este aspecto.

La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- Documentación de los procedimientos.





- Registro de incidencias.
- Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

Se deberá implementar un proceso de revisión continua con el fin de detectar vulnerabilidades en los procesos y sistemas. Estas revisiones deberán ser periódicas y realizarse al menos trimestralmente, poniendo a disposición de ICM los resultados de dichas revisiones. Al menos se deberán revisar las configuraciones de seguridad con intervalos no superiores a un trimestre, poniendo a disposición de ICM los resultados de dichas revisiones.

Las evaluaciones no deberán tener impacto en los servicios, y deberá informarse a ICM del inicio y finalización de las mismas y solicitar la autorización previamente a su realización.

CLÁUSULA 11.- PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será, como máximo, de **TREINTA Y SIETE MESES**, comprendidos entre el 1 de mayo de 2015 a 31 de mayo de 2018, de conformidad con los hitos que se detallan a continuación:

- **Fase de puesta en marcha del servicio**: Esta primera fase tendrá una duración, como máximo, de **1 mes**, comprendida entre el 1 y el 31 de mayo de 2015.
- **Fase de pleno servicio**: Esta fase tendrá una duración de **36 meses**, comprendidos entre el 1 de junio de 2015 y el 31 de mayo de 2018.

Transición de salida: tendrá una duración de **1 mes**, comprendido en el último mes de ejecución del contrato.

Si en la fecha de inicio de la ejecución, no se pudiera contar con la disponibilidad del equipo y medios necesarios para el inicio de los trabajos que constituyen el objeto del contrato, la Agencia de Informática y Comunicaciones de la Comunidad de Madrid quedará facultada para instar la resolución del contrato.

CLÁUSULA 12.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE ICM

El contratista no adquiere ningún derecho sobre el hardware (material), software e infraestructuras **propiedad de ICM**, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanadas del contrato.

El contratista **no podrá utilizar la información** obtenida en la actividad desarrollada como consecuencia del contrato, para fines distintos de los expresamente recogidos en el mismo, no pudiendo transmitir ni difundir dicho conocimiento o información, sin el consentimiento expreso y por escrito de ICM.



CLÁUSULA 13.- PRESUPUESTO BASE DE LICITACIÓN.

El **Presupuesto Base de Licitación** se ha establecido teniendo en cuenta la suma de los importes fijados para los servicios incluidos en cuota fija y los servicios de coste variable, según se detalla a continuación.

13.1 Servicios de Coste Fijo.

El presupuesto base de licitación estimado para los Servicios de Coste Fijo asciende a **519.740,64 €** IVA no incluido.

El volumen de certificados cuya emisión puede ser solicitada por ICM al adjudicatario, durante el plazo de ejecución del contrato, es el que se recoge en la siguiente tabla:

Tipo de CERTIFICADO	Nº de Certificados Solicitado
Certificados para el ciudadano que se relacione con la Administración Pública	Ilimitado
Certificados para personal al servicio de las Administraciones Públicas	Ilimitado
Certificados de persona jurídica	150
Certificados para la Identificación electrónica de las Sedes Electrónicas de la Comunidad de Madrid	2
Certificados de sello electrónico para la actuación administrativa automatizada	30
Certificados de componente	160

Al importe del presupuesto anteriormente indicado se le aplicará el porcentaje de baja ofertado por la empresa que resulte adjudicataria.

En relación al servicio de emisión, renovación, revocación y suspensión de Certificados para el personal al servicio de las Administraciones Públicas y de Certificados para el ciudadano, el número de certificados incluidos en la cuota fija será ilimitado y sin coste adicional.

La prestación de servicios contemplados en el apartado 4 del presente pliego distintos a la emisión de certificados electrónicos y soportes criptográficos, será ilimitada en cuanto a las transacciones, comunicaciones o consultas que puedan verificarse por ICM, y su coste está incluido en el presupuesto para los servicios de coste fijo.

13.2 Servicios de Coste Variable.

ICM se reserva el derecho de solicitar y obtener la prestación de servicios objeto del presente contrato **por encima del volumen** previsto en el apartado de costes fijos.



Los **importes unitarios** correspondientes a los **servicios de coste variable** serán los que resulten de aplicar el porcentaje de baja ofertado por la empresa que resulte adjudicataria a los importes que se señalan a continuación:

CERTIFICADOS DE PERSONA JURÍDICA	IMPORTES UNITARIOS
Hasta 10 certificados adicionales	96,00 €
Desde 11 hasta 30 certificados adicionales	72,00 €
A partir de 31	62,40 €

CERTIFICADOS DE SEDE ELECTRÓNICA	IMPORTES UNITARIOS
Hasta 10 certificados adicionales	305,09 €
Desde 11 hasta 30 certificados adicionales	244,07 €
A partir de 31	152,54 €

CERTIFICADOS DE SELLO ELECTRÓNICO	IMPORTES UNITARIOS
Hasta 100 certificados adicionales	195,25 €
Desde 101 hasta 150 certificados adicionales	152,54 €
A partir de 151	109,82 €

CERTIFICADOS DE COMPONENTE	IMPORTES UNITARIOS
Hasta 150 certificados adicionales	109,82 €
Desde 151 hasta 200 certificados adicionales	79,32 €
A partir de 201	54,91 €

SOPORTES CRIPTOGRÁFICOS	IMPORTES UNITARIOS
1 Tarjeta	5,00 €

AMPLIACIÓN REGISTRO MÓVIL (coste hora)	IMPORTES UNITARIOS
1 Registrador Adicional	35,12 €

DESARROLLO DE SERVICIOS BAJO DEMANDA (coste hora)	IMPORTES UNITARIOS
Precio / Hora	34,34 €

El importe máximo correspondiente a los Servicios de Coste Variable, (36 meses), será el que resulte de aplicar el porcentaje de baja ofertado por la empresa que resulte adjudicataria a **224.995,25 €**, IVA no incluido, que se abonará en el caso de que ICM demande la prestación de servicios adicionales a los contemplados en el apartado 1 de la presente Cláusula (Servicios de Cuota Fija) y por los precios unitarios anteriormente referidos.



CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente Pliego de Cláusulas Técnicas, los licitadores deberán remitir por correo electrónico las preguntas e información que consideren necesarias, a la siguiente dirección de correo: icm_seguridad_sistemas@madrid.org. Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con ICM, para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente Pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada. Así mismo los licitadores para formular sus consultas o aclaraciones deberán cumplimentar la siguiente plantilla:

Nº cuestión	Capítulo/Apartado	Página	Párrafo	Descripción de la consulta
-------------	-------------------	--------	---------	----------------------------

Por su parte ICM, se compromete a responder con la suficiente antelación, distribuyendo, entre todos los licitadores, todas las respuestas a las consultas y aclaraciones efectuadas, sin identificar la procedencia de ellas.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1000031128665707605074**

ANEXO

**AL PLIEGO DE CLAUSULAS TÉCNICAS QUE HAN DE REGIR EN EL CONTRATO DE SERVICIOS
DENOMINADO “SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA”, A ADJUDICAR POR PROCEDIMIENTO
SIMPLIFICADO ORDINARIO MEDIANTE PLURALIDAD DE CRITERIOS**

MODELO DE CURRÍCULUM

(A aportar para cada miembro del equipo de trabajo propuesto)

APELLIDOS:	
NOMBRE:	

CATEGORÍA PROFESIONAL:

TITULACIÓN / UNIVERSIDAD o CENTRO / HOMOLOGACIÓN (en caso de haberse obtenido la titulación fuera de España):

FORMACIÓN:

ACTIVIDAD PROFESIONAL (especificando como mínimo: empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta):

NOTAS:

La empresa propuesta como adjudicataria, con carácter previo a la adjudicación, deberán aportar este documento, debidamente cumplimentado y firmado por la persona que ostente la representación de la empresa, para cada uno de los miembros del equipo propuesto, indicando el perfil al que se adscribe, así como toda aquella documentación que ICM estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

Fecha y firma

El Consejero-Delegado de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid

Fdo.: Blas Labrador Román

