

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EN EL
CONTRATO DE SERVICIOS DENOMINADO “SERVICIO DE RED DE
DISTRIBUCIÓN DE CONTENIDOS (CDN) PARA EL PORTAL
WWW.MADRID.ORG”**



INDICE

| | | |
|----------------------|--|-----------|
| CLÁUSULA 1.- | ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD | 3 |
| CLÁUSULA 2.- | OBJETO DEL CONTRATO | 4 |
| CLÁUSULA 3.- | REQUERIMIENTOS | 4 |
| CLÁUSULA 4.- | TRABAJOS A REALIZAR | 8 |
| CLÁUSULA 5.- | VOLUMETRIA..... | 8 |
| CLÁUSULA 6.- | NIVELES DE SERVICIO Y PENALIZACIONES | 9 |
| CLÁUSULA 7.- | INCIDENCIAS Y SOPORTE | 9 |
| CLÁUSULA 8.- | RESPONSABLE DEL SERVICIO..... | 11 |
| CLÁUSULA 9.- | ESTRUCTURA NORMALIZADA DEL CONTENIDO DE LAS OFERTAS | 12 |
| CLÁUSULA 10.- | SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO | 13 |
| CLÁUSULA 11.- | GESTIÓN DE LA SEGURIDAD | 14 |
| 11.1.- | Introducción | 14 |
| 11.2.- | Protección de datos de carácter personal | 15 |
| 11.3.- | Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica | 20 |
| 11.4.- | Propiedad de los trabajos..... | 20 |
| 11.5.- | Derechos sobre el hardware, software e infraestructuras de ICM | 21 |
| 11.6.- | Restricciones generales..... | 21 |
| 11.7.- | Auditoría de la seguridad y trazabilidad de los servicios | 22 |
| CLÁUSULA 12.- | PLAZO DE EJECUCIÓN | 23 |
| CLÁUSULA 13.- | CONSULTAS SOBRE EL PLIEGO DE CLAUSULAS TECNICAS | 23 |



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **0944909867483792499266**

CLÁUSULA 1.- ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

La Agencia de Informática y Comunicaciones de la Comunidad de Madrid (en adelante ICM), según *Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas* (BOCM Núm. 311, de 30 de diciembre de 2005), tiene asignada, entre otras funciones, 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, el desarrollo y adquisición de aplicaciones informáticas y sistemas de información para la Comunidad de Madrid, y su mantenimiento y soporte posteriores, de acuerdo con las especificaciones funcionales y necesidades de los distintos centros directivos (*Artículo 10 Tres c) 2.º*). En su virtud es competencia de esta Agencia la contratación de los servicios que a continuación se detallan.

En el ejercicio de sus funciones ICM tiene entre sus competencias garantizar una mejor prestación de los servicios ofrecidos a los ciudadanos de la Comunidad de Madrid, mediante la ampliación y mejora de los sistemas de información.

A tal fin, esta Agencia está realizando una apuesta de futuro en nuevas tecnologías para proporcionar al ciudadano la mejor información y calidad en los servicios prestados a través del portal www.madrid.org, con intención, además, de convertirlo en una referencia nacional e internacional.

Para la Comunidad de Madrid, el portal “**madrid.org**”, es el punto de acceso por el canal web a ciudadanos y empresas a los servicios de consulta de información, realización de trámites telemáticos de envío y recepción de escritos, solicitudes, documentos y cualquier otra operación reflejada como derecho en la ley 11/2007, de 22 junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

En el caso de la Comunidad de Madrid se ha realizado un esfuerzo muy grande para dotar a su portal institucional, “**madrid.org**”, de toda la información y servicios de utilidad a ciudadanos y empresas, siendo creados nuevos contenidos de forma continua y siendo éstos constantemente actualizados.

Ello supone que el volumen de contenidos del portal es muy alto y que a su vez el número de visitas y páginas vistas es también muy elevado.

Por tanto el sistema elegido para hacer llegar los contenidos web a ciudadanos y empresas debería ser capaz de soportar cargas elevadas de trabajo, absorbiendo cualquier volumen de tráfico, en modelo 24x7 y por supuesto, con independencia de las condiciones de Internet, tanto en tráfico como en rendimiento.



Adicionalmente, debería ser un requisito imprescindible que la Comunidad de Madrid conserve en todo momento el control del portal, incluyendo la metodología de publicación, la capacidad de refresco de contenidos, el reporte de actividad en tiempo real y la información ejecutiva histórica. La degradación en el rendimiento, en la fiabilidad o en la escalabilidad del portal, afecta negativamente en la experiencia de navegación del usuario, impactando negativamente en la imagen que la Comunidad de Madrid da a ciudadanos y empresas y en lo que es más importante en la calidad de la prestación de servicios.

Se busca un servicio que nos proporcione la funcionalidad básica de entrega de contenidos Web de forma fiable e independiente de las infraestructuras que la Comunidad de Madrid tiene para el portal www.madrid.org.

El objetivo es garantizar en cualquier situación, la disponibilidad del portal en el entorno Internet. El servicio de aceleración dinámica de contenidos web, actuaría como intermediario en lo que se refiere a infraestructuras, en la provisión del servicio Web, asegurando un rendimiento correcto en los momentos de máxima concurrencia de accesos y actividad del portal.

CLÁUSULA 2.- OBJETO DEL CONTRATO

La prestación del servicio de red de distribución de contenidos (CDN) para la entrega de contenidos del portal “www.madrid.org” con el fin de asegurar la disponibilidad del portal institucional en todo momento y bajo unos niveles óptimos de calidad en la prestación del servicio, de conformidad con los requerimientos establecidos en el presente pliego.

CLÁUSULA 3.- REQUERIMIENTOS

Una red de distribución de contenidos (más conocida por sus siglas en inglés Content Delivery Network o CDN), es un servicio de red que facilita la distribución de información generada por los editores. Para cumplir este objetivo, se distribuyen servidores geográficamente, de forma que el contenido esté más cercano a los usuarios, pasando de un modelo centralizado a un modelo mixto, donde la publicación se realiza de forma centralizada, pero la difusión de la información utiliza un servicio proporcionado por terceros, que es el objeto del presente pliego. La CDN debe permitir la entrega de contenido a través del protocolo http y hacer “stream” de video en varios formatos y protocolos.



Los requisitos de **obligado cumplimiento** para el servicio son los siguientes:

1. **Cache HTTP:** El contenido debe ser almacenado en el servicio CDN. Para ello el adjudicatario debe proporcionar al menos dos posibilidades de hacerlo:
 - a. Recuperándolo de los servidores indicados por la Agencia
 - b. Proporcionando un origen en la propia CDN donde la Agencia podrá subir el contenido a través de protocolos estándar (FTP, SFTP, http, etc.). Deberá poder subirse contenido de cualquier tipo multimedia.

El contenido debe ser cacheado en función de unas reglas, que permitan al menos lo siguiente:

- a. A través de expresiones regulares, indicando individualmente por cada URL el tiempo de permanencia en cache
- b. El número de reglas a definir es variable, por tanto el número de reglas permitidas por la CDN debe ser lo suficientemente flexible para permitir cachear todo lo que precise la Agencia
- c. Debe permitir obviar lo que indiquen las cabeceras enviadas por los servidores de origen (principalmente 'cache-control' y 'expires')
- d. Caducar en cualquier momento (24x7x365) contenido subido a la CDN
- e. Subir contenido a la CDN en 24x7x365
- f. Permitir indicar páginas específicas ante códigos de error
- g. La mayoría de las peticiones a cachear tendrán un formato similar al siguiente:

http://www.madrid.org/cs/Satellite?pagename=ComunidadMadrid/Estructura&cid=11232123123123&c=CM_Test_FA&lang=es

Una vez el contenido esté almacenado en la caché, deberá servirse desde ahí hasta que caduque según el TTL (Time-to Live) especificado, momento en el cual debe volver a solicitarse al origen. Si éste no estuviera disponible, deberá servirse el antiguo hasta que el nuevo esté disponible.

Los tipos de contenido que el sistema almacenará en su caché serán:

- Objetos web
- Objetos para descargar (archivos multimedia, software, documentos)
- Aplicaciones
- Streaming



La Agencia indicará qué portales deben servirse mediante la CDN y se encargará de su configuración junto con el proveedor del servicio. Cada portal, puede estar configurado en un dominio diferente a www.madrid.org. El número de dominios, por tanto, será variable, y la inclusión de nuevos dominios no debe suponer un coste adicional siempre que no se superen los parámetros establecidos en el dimensionamiento del servicio en cuanto a ancho de banda, páginas vistas y volumen estimado de almacenamiento.

2. **Video bajo demanda (Streaming):** Uno de los tipos de contenidos que pueden subirse a la CDN son videos. Ésta permitirá su descarga mediante el protocolo http (http progresivo).
3. **Generación de Web Estática:** La mayor parte del contenido que se genera en el portal www.madrid.org y portales asociados es dinámico, lo cual implica que hay publicaciones constantes que precisan de una infraestructura compleja en la que un fallo puede dejar sin servicio al portal. Para mitigar cualquier problema, se precisa disponer de una copia estática, a modo de “fotografía” del portal en un instante dado, descargable en un sistema de ficheros, y que permita la navegación por el portal de forma estática a través de los ficheros descargados. Se asume que hay funcionalidades que dejarían de funcionar, relacionadas con el contenido a generar mediante formularios o buscadores. La generación de la web deberá controlarse desde la consola de administración del servicio. Una vez programada la generación, ésta se realizará de forma automática sin intervención de operadores.
4. **Conmutación ante fallos:** La CDN almacenará el contenido en sus servidores de cache y lo servirá desde ahí hasta que este contenido caduque, momento en el que se conectará al servidor de origen para recuperar el nuevo contenido. Si por cualquier motivo fuera imposible recuperar este contenido, y no tuviera copia de lo que tiene que servir en su cache, se conectará a la web estática generada para recuperarlo. A través de este modo de funcionamiento, el portal siempre estará disponible para los usuarios.
5. **Seguridad:** El adjudicatario de la CDN debe proporcionar servicios de seguridad que permitan detectar y mitigar (dada la imposibilidad técnica de prevenirlos o eliminarlos) los siguientes tipos de ataque:
 - a. Ataques de denegación de servicio, siendo capaz de procesar el tráfico generado.
 - b. Ataques a través de URLs (inyección de código): Mediante patrones de detección, detectará posibles vectores de ataque generando alertas y permitiendo tomar medidas de defensa.



6. **Consola de administración:** Se debe proporcionar una consola de administración, accesible via http/https, que permita configurar completamente el servicio y controlar el estado de éste, a través de gráficas e informes.
7. **Alertas:** El servicio debe poder permitir la configuración de alertas en tiempo real mediante criterios definidos por la agencia sobre el funcionamiento de éste. El mecanismo de notificación será preferente por email y opcionalmente por SMS.
8. **Informes:** Se generarán informes estadísticos en base a los datos registrados por los servidores de la CDN. Se proporcionarán al menos informes sobre el ancho de banda consumido, número total de peticiones, páginas de error, distribución de la carga en el tiempo, etc. Los informes deberán poder generarse bajo demanda o permitir la programación de envíos periódicos.
9. **Servicios de Soporte:** Estará incluido en el contrato los servicios de soporte necesarios que permitan resolver las incidencias y consultas que surjan durante la prestación del servicio. La descripción detallada de los servicios requeridos se detallan en la cláusula 7.

Todas las funcionalidades requeridas deben proporcionarse en un nivel de calidad que aseguren las siguientes características:

- **Disponibilidad:** Alta disponibilidad del sitio web y todos sus contenidos en cualquier circunstancia. Dentro del servicio debe estar incluida la capacidad de entregar el último contenido válido en caso de indisponibilidad de origen, y aún más allá, disponer de una copia estática, en caso de no existir almacenado en la plataforma dinámica ningún contenido.
- **Escalabilidad:** la plataforma ha de absorber en cada momento cualquier volumen de tráfico, sin límite de infraestructura ni de ancho de banda.
- **Rendimiento:** el rendimiento del sitio web para cada usuario final debe ser óptimo,



CLÁUSULA 4.- TRABAJOS A REALIZAR

El licitador deberá realizar los trabajos objeto de este contrato en un plazo de 24 meses, estableciéndose las siguientes fases:

- **FASE 1 (3 semanas):** Diseño y plan de trabajo. En esta fase se consensuará con la Agencia la propuesta presentada, la planificación detallada de actividades y la configuración necesaria para la puesta en funcionamiento del servicio. Deberá contemplar en las actividades la generación de una web estática y la migración de los contenidos almacenados en el anterior proveedor.
- **FASE 2 (hasta el final del contrato):** Prestación del servicio. Se prestará el servicio en los términos expuestos en la cláusula 3.

Como entregables de trabajos se considerarán los siguientes:

- **Entregables Fase 1:**
 - a) Documento de Diseño del servicio
 - b) Documento de planificación
 - c) Migración de contenidos al proveedor
 - d) Construcción de una web estática y guía de configuración
 - e) Documento de gestión de cambios en el servicio
- **Entregables Fase 2:**
 - a) Informes de seguimiento del servicio

CLÁUSULA 5.- VOLUMETRIA

Los volúmenes de información, ancho de banda y capacidad de almacenamiento en condiciones normales de servicio requeridos a la CDN, se enumeran a continuación:

- Tráfico diario servido desde la CDN: 600 Gb +/- 10%
- Distribución del tráfico: 200 Mbits/s en franjas pico
- Páginas diferentes: 1.5 Millones
- Volumen de almacenamiento requerido: **1Tb**.



CLÁUSULA 6.- NIVELES DE SERVICIO Y PENALIZACIONES

La disponibilidad exigida al servicio CDN será igual o superior al **99,995%** medida mensualmente. Para la medición se utilizarán sondas que comprobarán el estado del servicio de forma continua. Se entenderá por indisponibilidad, la imposibilidad del acceso al portal www.madrid.org por los ciudadanos, por causas imputables al adjudicatario del servicio. Para la medición se utilizarán servicios de terceros y sondas propias de la Agencia.

El servicio debe prestarse con una disponibilidad mayor del 99,995%. En caso de incumplimiento del nivel exigido se aplicará una penalización económica por tramos según se especifica en el siguiente cuadro:

| Tramo | Disponibilidad | Penalización |
|-------|-----------------------|--------------|
| T1 | 99,671%<Disp<=99,741% | 4% |
| T2 | 99,741%<Disp<=99,982% | 3% |
| T3 | 99,982%<Disp<=99,995% | 2% |
| T4 | 99,995%<Disp | 0% |

La medición de la disponibilidad se realizará de forma mensual y las penalizaciones se aplicarán en el siguiente mes de facturación en el que se produjeron.

CLÁUSULA 7.- INCIDENCIAS Y SOPORTE

Con carácter general, los Servicios de Atención y Soporte de los **Sistemas de Información de la Comunidad de Madrid** se estructuran en 3 niveles de gestión:

- **Nivel 1:** Atención y Soporte a Usuarios Generales
- **Nivel 2:** Servicio Técnico general de soporte
- **Nivel 3:** Servicio Técnico especializado, ofrecido normalmente por el proveedor

Los niveles 1 y 2 quedan fuera del ámbito de aplicación de este contrato.



Soporte Técnico Especializado (Nivel 3):

El objetivo de este nivel es proporcionar un servicio integral de soporte al servicio referido en este contrato. Este soporte cubrirá los siguientes puntos:

- Atención y resolución de Incidencias y peticiones de información
- Acceso a personal de la Agencia a las herramientas de configuración y pruebas
- Contacto mediante correo electrónico, telefónico o canal web con el equipo de soporte indicado
- Los **tiempos de respuesta** para las incidencias se establecen de la siguiente manera:
 - a. Incidentes **Críticos**: Máximo 2 horas
 - b. Incidentes **Graves**: Máximo 4 horas
 - c. Incidentes **Leves**: Máximo 2 días laborables
- Los incidentes críticos deberán contar con soporte 24x7 y se notificarán vía telefónica
- En eventos especiales (elecciones principalmente) se requerirá soporte 24x7 el día del evento.
- La puesta en marcha del servicio se considera parte del soporte. Esta puesta en marcha debe cubrir aspectos tales como la configuración del servicio, la utilización de herramientas específicas del proveedor, documentación, gestión de problemas, resolución de dudas. Cualquier problema que surja durante el periodo de activación debe estar cubierto.

Clasificación de Incidentes:

| Impacto | Tiempo de Respuesta | Descripción |
|---------|---------------------|---|
| Crítico | 2 horas | El servicio está detenido y hay multitud de usuarios con problemas de acceso. El número de usuarios afectados es alto |
| Grave | 4 horas | Problemas de utilización de servicio desde alguna localización concreta. El número de usuarios afectados es bajo |
| Leve | 2 días laborables | Peticiones de información, consultas sobre cambios de configuración, informes. |



Horarios de Servicio y Tiempo de Respuesta:

El **tiempo de respuesta** se define como el tiempo transcurrido entre el momento en que se notifica la incidencia y el momento en que un técnico de la empresa adjudicataria realiza la primera comunicación, según los canales establecidos, informando sobre el análisis de las causas de la incidencia y las acciones correctivas a realizar, con los plazos en los que se llevarán a cabo.

Para el cómputo de tiempos hay que tener en cuenta las siguientes consideraciones:

- **Días laborables:** Son todos los días de la semana de lunes a viernes, excepto sábados y festivos, según el calendario laboral de Madrid-capital, en horario de 8:00 a 17:00
- **Periodos de cumplimiento en días laborables:** Cuando el tiempo especificado es en días laborables, se refiere al tiempo transcurrido desde que ICM notifica el aviso al adjudicatario hasta la última hora del día en que finaliza el plazo.
- **Periodos de cumplimiento en horas:** Dado que el soporte requerido para incidencias críticas, debe considerarse en periodo 24x7, las horas contarán desde que se notifica la incidencia.

CLÁUSULA 8.- RESPONSABLE DEL SERVICIO

El adjudicatario designará un **Responsable del Servicio ante ICM** y se encontrará en permanente contacto con el personal de ICM designado por la Dirección de la Agencia, deberá tener la siguiente cualificación técnica:

- Categoría Profesional mínima: Licenciado Superior, Grado o equivalente.
- Actividad Profesional mínima: Se deben acreditar, al menos, tres años de actividad profesional realizando labores de jefe de proyecto.

Se aportará **Curriculum Vitae del Responsable del Servicio ante ICM propuesto para la ejecución del contrato**, según el *Modelo* incluido en el Anexo I al Pliego de Cláusulas Técnicas, debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional (con detalle de *perfil técnico, titulación, formación y actividad profesional*), así como toda aquella documentación que ICM estime necesaria para la acreditación de los datos contenidos en dicho Currículum, según se señala en la **Cláusula 14** del Pliego de Cláusulas Jurídicas.



El adjudicatario, a través del Responsable del Servicio y con la periodicidad que ICM determine, informará sobre la planificación de trabajos, estado de ejecución del contrato y si procede, de las incidencias producidas.

Las tareas a realizar serán las siguientes:

- Coordinar el apoyo técnico en aquellas materias necesarias para la prestación del servicio
- Gestionar la planificación de peticiones que realice ICM
- Supervisar y controlar el servicio
- Gestionar los cambios en el servicio
- Asumir la responsabilidad final sobre el funcionamiento del servicio

CLÁUSULA 9.- ESTRUCTURA Y CONTENIDO MINIMO DE LAS OFERTAS

En la presente cláusula se describe la estructura según la cual deberán elaborarse las ofertas técnicas presentadas por los licitadores. Para la elaboración de la oferta, los licitadores deberán basarse en los requerimientos recogidos en el presente pliego.

La exposición de la oferta técnica propuesta se ajustará como mínimo y en su mismo orden a los apartados detallados a continuación. Con carácter obligatorio, la propuesta deberá presentarse en papel y en soporte informático, compatible con las herramientas instaladas en ICM (MS Word, Adobe Acrobat Reader).

El licitador deberá ajustarse especialmente a lo indicado en esta cláusula y circunscribir su propuesta exclusivamente a lo demandado en el pliego, separando claramente en la documentación que entregue lo aplicable íntegramente como respuesta técnica, evaluable, de la información sobre catálogos de servicios, especificaciones técnicas y condiciones de servicio que se deberán incluir como anexos a la oferta.

Las ofertas deberán ajustarse al siguiente contenido y formato:



- Índice
- Infraestructura Tecnológica: Características técnicas de la infraestructura que dará soporte al servicio requerido. Se incluirá toda la información relevante que permita clasificar el servicio de red ofrecido, atendiendo a sus características de composición de la CDN, forma de gestionar y distribuir el contenido, aceleración de peticiones, y medición del rendimiento
- Descripción de la solución técnica: Se incorporará al inicio de este apartado el resumen ejecutivo de los aspectos más significativos y relevantes de la solución ofertada.
- Detalle de la solución técnica, ajustándose en la medida de lo posible al pliego de Prescripciones Técnicas:
 - a. Requerimientos
 - b. Volumetría
 - c. Soporte e Incidencias
 - d. Guía de realización de copias estáticas

| |
|---|
| CLÁUSULA 10.- SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO |
|---|

El seguimiento y control de los servicios a prestar por parte del adjudicatario, se efectuará sobre las siguientes bases:

- Seguimiento continuo de la evolución del servicio entre el Responsable del Servicio por parte del adjudicatario y el Responsable del Contrato que ICM designe.
- ICM determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control del servicio.



CLÁUSULA 11.- GESTIÓN DE LA SEGURIDAD**11.1.- Introducción**

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 al mantenimiento y desarrollo de aplicaciones, 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 de las actividades relacionadas a continuación, así como al mantenimiento de los registros de evidencias del cumplimiento de las mismas durante al menos todo el periodo de ejecución del contrato:

- Definir, implementar y mantener una política de seguridad.
- Identificar e implantar las medidas de seguridad dimanantes de la normativa relacionada anteriormente con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información de la Comunidad de Madrid, en respuesta a los requisitos especificados en este clausulado. Para ello, se deberá realizar un estudio al inicio de los trabajos para identificar las medidas de seguridad que apliquen respecto al nivel de seguridad de cada aplicación y utilizar la guía interna de ICM para implementar y documentar las medidas de seguridad aplicables en la fase de desarrollo del software.
- 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.

Los siguientes apartados establecen las condiciones y medidas en materia de seguridad que el adjudicatario deberá implantar y mantener para la prestación de los servicios. 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 a la legislación vigente y al cuerpo normativo de seguridad de ICM.



11.2.- 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 Persona, en adelante LOPD.

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.
 - 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 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 1.1, 1.2 y 1.3, 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 1.2); 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 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 la *letra c) del apartado Tres del artículo 10 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 Real Decreto 1720/2007, de 21 de diciembre, 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, 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 **ADJUDICATARIOS**, 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*.

11.3.- Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica

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.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán de forma obligatoria las medidas de seguridad indicadas en su anexo II pertenecientes al marco organizativo. Respecto a los marcos operacional o de protección, se estará a lo establecido en la declaración de aplicabilidad del objeto de este contrato, en su caso.

El Documento de Seguridad reflejará, además de lo estipulado con carácter general en el apartado Documentación de Seguridad, 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.

11.4.- Propiedad de los trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del contrato serán propiedad de ICM, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego, 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 desarrolladas al amparo del contrato, corresponden únicamente a la Comunidad de Madrid y, particularmente, a ICM.



11.5.- 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.

11.6.- Restricciones generales

En el marco de la ejecución del contrato, y respecto a los sistemas de información de ICM que le den 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.

11.7.- 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:

- a) Documentación de los procedimientos.
- b) Registro de incidencias.
- c) 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 12.- PLAZO DE EJECUCIÓN

El plazo de ejecución será de **VEINTICUATRO MESES**, desde el **desde el 1 de Agosto de 2015 al 31 de Julio de 2017**

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 13.- CONSULTAS SOBRE EL PLIEGO DE CLAUSULAS TECNICAS

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 podrán dirigirse a:

*Agencia de Informática y Comunicaciones de la Comunidad de Madrid
C/ Embajadores, 181. 28045 – Madrid
Dirección de Servicios a Clientes de Presidencia, Educación, Transportes
y de Administración Electrónica
Área de Difusión Electrónica
Teléfono 915805000
Horario: 09h a 18 h. (Lunes a Viernes)*



ANEXO I: MODELO DE CURRÍCULUM VITAE

(A aportar por cada miembro del equipo base de trabajo propuesto)

| | |
|--|--|
| APELLIDOS: | |
| NOMBRE: | |
| CATEGORÍA PROFESIONAL: | |
| TITULACIÓN: | |
| FORMACIÓN: | |
| ACTIVIDAD PROFESIONAL (especificando, como mínimo, Empresa, Duración del proyecto, Descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta): | |

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

Fdo.: Blas Labrador Román



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **0944909867483792499266**