

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DENOMINADO “DEFINICIÓN Y DESARROLLO DEL MODELO ORGANIZATIVO Y FUNCIONAL DE CIBERSEGURIDAD DE LA AGENCIA PARA LA ADMINISTRACIÓN DIGITAL DE LA COMUNIDAD DE MADRID”, A ADJUDICAR MEDIANTE PROCEDIMIENTO SIMPLIFICADO ORDINARIO CON PLURALIDAD DE CRITERIOS

CLÁUSULA 1.- INTRODUCCIÓN

Tras la entrada en vigor del **Artículo 4** de la **Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas** (BOCM Núm. 311, de 31 de diciembre de 2015), que modifica parcialmente el **Artículo 10** de la **Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas**, la Agencia de Informática y Comunicaciones de la Comunidad de Madrid pasa a denominarse **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante **Madrid Digital**), manteniendo su naturaleza, así como sus funciones, recogidas en el precitado Artículo 10, Tres, c), entre las cuales se encuentra la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, y en concreto:

1. 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.
2. 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.
3. La adquisición y dotación de infraestructuras físicas y lógicas de soporte de los sistemas de información de la Comunidad de Madrid, y de sus servicios.

En la actualidad las Administraciones Públicas y, en particular, la Comunidad de Madrid, han apostado firmemente por un impulso de la transformación digital en su oferta de servicios al ciudadano, siendo ésta clave en los objetivos a alcanzar en la presente legislatura.

La Agencia para la Administración Digital de la Comunidad de Madrid tiene asignadas, entre otras funciones (además de las enumeradas más arriba), las siguientes:

- El control del cumplimiento de la normativa a que deberán atenerse los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones desarrollados o adquiridos por la Comunidad de Madrid, a fin de asegurar su utilidad y compatibilidad.
- El aseguramiento de la integración efectiva en la infraestructura física y lógica gestionada por la Agencia, y la adecuación a los estándares y normativa aplicable, de todos aquellos sistemas materiales o lógicos relativos a la informática y las comunicaciones que hubieran sido o fueran en el futuro transferidos a la Comunidad de Madrid desde otras entidades estatales o locales, en cualquier ámbito.
- La elaboración de la normativa e instrucciones para la utilización de los diferentes equipamientos por los usuarios.
- La seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad.



A tal fin, Madrid Digital ya recoge como objetivo en su *Política de Seguridad* el cumplimiento de las siguientes directrices de seguridad:

- Establecer los requisitos de seguridad de obligado cumplimiento para el personal interno y externo a la Agencia, así como para los activos de su propiedad o custodiados por ella.
- Estructurar un marco de gestión y organización de la seguridad donde se asignen responsabilidades y tareas relacionadas con la seguridad.
- Establecer el alcance de los controles que se precisan para cumplir con las necesidades de seguridad a nivel corporativo.
- Impulsar el establecimiento sistemas de gestión de seguridad de la información para los procesos de la Agencia.

La ciberseguridad ha sido contemplada, en este proceso de transformación, como una de las líneas claves en las que se debe prestar todos los esfuerzos necesarios de forma que se aporte la confiabilidad adecuada de los servicios que la Administración ofrece al ciudadano a través de las Tecnologías de la Información y la Comunicación (en adelante TIC).

Por otro lado, se viene produciendo en ámbito de actuación de todas las Administraciones Públicas un cambio de paradigma en el concepto y entendimiento del modelo de la seguridad, que está evolucionando desde el enfoque clásico de seguridad defensiva a otro de ciberseguridad donde debe primar la prevención, anticipación, vigilancia, rápida respuesta y reacción ante incidentes y la mejora de la resiliencia de las tecnologías de la información y las comunicaciones.

Por todo ello, Madrid Digital se ha planteado realizar un análisis interno de su modelo de gobierno y operación de la seguridad para definir y desarrollar un nuevo modelo de capacidades y funciones de seguridad orientado al nuevo enfoque de la ciberseguridad que se plantea actualmente.

CLÁUSULA 2.- OBJETO

La prestación de los servicios de consultoría para elaborar el modelo organizativo y funcional de ciberseguridad de Madrid Digital, mediante el análisis de la actividad de la Agencia en materia de seguridad, establecimiento del nuevo modelo de gestión de la ciberseguridad, análisis posicional GAP, catálogo de nuevos servicios de ciberseguridad y planificación de los nuevos proyectos.

CLÁUSULA 3.- ALCANCE

El alcance de los trabajos a desarrollar incluye los siguientes:

- Análisis de los servicios ofrecidos por Madrid Digital a la Administración de la Comunidad de Madrid y al ciudadano.
- Análisis de la organización interna de Madrid Digital y la asignación de las competencias de cada una de sus Unidades Organizativas.
- Propuesta del modelo organizativo y de capacidades de ciberseguridad de Madrid Digital, que deberá estar basado en estándares reconocidos en la materia.
- Desarrollo del detalle de los procesos y servicios de ciberseguridad soportados en cada una de las capacidades definidas bajo el modelo de ciberseguridad de Madrid Digital, así como el detalle de los roles, funciones y responsabilidades de sus Unidades organizativas.



- Análisis GAP, identificando los controles para determinar del grado de madurez de las capacidades actuales de Madrid Digital frente a las recogidas en el modelo objetivo propuesto.
- Elaboración y desarrollo del plan de ciberseguridad donde se recoja la hoja de ruta para la puesta en marcha e implantación del modelo de ciberseguridad de Madrid Digital.

CLÁUSULA 4.- DESCRIPCIÓN DE LOS SERVICIOS

Los trabajos que deberá desarrollar el adjudicatario son:

- **Identificar las capacidades** de Madrid Digital en materia de gestión de la ciberseguridad así como analizar y documentar las actividades que actualmente realiza la Agencia en este ámbito de competencias.
- **Diseñar y desarrollar un nuevo Modelo de Capacidades y de Prestación de Servicios de Ciberseguridad** para la Agencia Madrid Digital que determine y asigne a sus Unidades Organizativas **los nuevos roles y las nuevas responsabilidades** que resulten del modelo. Este nuevo modelo responderá a las demandas de servicios de ciberseguridad propias del contexto globalizado en el que se desenvuelven hoy en día los servicios y tecnologías TIC.
- **Realizar un análisis posicional (análisis GAP)** que determine el estado actual de desempeño de la Agencia en materia de ciberseguridad en relación con el nuevo modelo, así como la determinación del grado de madurez de la prestación de estos servicios a sus clientes y usuarios, así como a los ciudadanos.
- Elaborar un **Plan de Proyectos de desarrollo de la ciberseguridad** para Madrid Digital que incluya la identificación y descripción detallada de todos los trabajos que la Agencia precisa acometer para estar en disposición de ofrecer nuevos servicios de ciberseguridad, según los umbrales de madurez que se hayan concretado previamente.
- Realizar **workshops para el apoyo y soporte a las tomas de decisiones** en la definición de servicios de ciberseguridad y en la asignación de roles y responsabilidades de las Unidades Organizativas de Madrid Digital para prestarlos.
- Realizar las **presentaciones ejecutivas** del avance y de resultados a la Dirección de Madrid Digital.

El adjudicatario deberá abordar el análisis de la siguiente forma:

- 1) Dividirá el planteamiento general de la ciberseguridad en **cuatro ámbitos**, que serán los siguientes:
 - a) **Gobierno**
 - b) **Prevención**
 - c) **Detección**
 - d) **Respuesta y recuperación**

A partir de estos cuatro ámbitos generales, el adjudicatario desarrollará todo el modelo organizativo y funcional de capacidades y de prestación de servicios de ciberseguridad de la Agencia.

- 2) Para cada uno de los cuatro ámbitos anteriormente señalados, el adjudicatario enumerará, definirá y desarrollará documentalmente el conjunto de **capacidades de gestión** que determine como necesarias para dar respuesta a las demandas de



servicios de ciberseguridad que tiene planteadas la Agencia, tanto para el momento actual como para el inmediato futuro.

- 3) Para cada una de las capacidades de gestión definidas se establecerá y documentará el **conjunto de servicios** ⁽¹⁾ que la Agencia, a través de las Unidades Organizativas que la componen, debe prestar, tanto internamente a su personal, como externamente, a sus clientes y usuarios, y a los ciudadanos.

El adjudicatario deberá organizar los trabajos según las siguientes **fases**:

Fase 1 – Planificación preliminar de los trabajos y análisis de la actividad de la Agencia en materia de seguridad. (Duración estimada: 4 semanas).

Dentro de esta fase se realizarán las siguientes tareas:

- a) El adjudicatario presentará, al inicio del contrato, un **Plan de Trabajo** detallado que deberá ser aprobado, antes de su puesta en marcha, por la Dirección de Seguridad Corporativa (en adelante, DSC), que actuará como Dirección del Proyecto. El plan de trabajo deberá contener, como mínimo, lo siguiente:
- Cronograma temporal con la duración de cada una de las fases y la descripción de los trabajos que comprende el proyecto.
 - Estructura, descripción completa y ejemplos de todos los modelos documentales a emplear a lo largo del proyecto.
 - Agenda de reuniones con las Unidades Organizativas de la Agencia con competencias en materia de seguridad ⁽²⁾.
 - Fechas de entrega previstas para cada uno de los documentos finales del proyecto.
 - Calendario de reuniones de seguimiento con la Dirección del Proyecto.
 - Estimación de holguras temporales.
- b) Un **análisis en profundidad** de la actividad que desarrollan las diferentes Unidades Organizativas **de la Agencia** con competencias **en seguridad**, en el que se prestará especial atención al entendimiento del modelo actual de desempeño de la Agencia y al grado de implementación real de este tipo de servicios.

El análisis tendrá por objetivo entender y documentar la distribución de competencias, las capacidades de servicio, el nivel de respuesta y la delimitación de responsabilidades que existen actualmente en la Agencia en materia de seguridad. El adjudicatario deberá alcanzar un grado de conocimiento de la Organización lo suficientemente elevado como para poder establecer posteriormente un modelo de gestión de la ciberseguridad que sea coherente con la actividad real de la Agencia, su estructura interna y su misión corporativa. Deberá asimismo documentar el grado de adecuación de los servicios de seguridad que actualmente presta la Agencia con la realidad de la demanda actual, en esta materia, de los clientes, usuarios y ciudadanos.

El adjudicatario documentará con el suficiente detalle la estructura actual de gestión de la seguridad en la Agencia Madrid Digital.

¹ La Agencia Madrid Digital estima que para que un *Modelo de Capacidades y de Prestación de Servicios de Ciberseguridad* pueda considerarse completo debe definir y documentar al menos un número no inferior a veinte (20) servicios.

² La agenda para estas reuniones se establecerá conjuntamente con la Dirección de Seguridad Corporativa.



No se dará por finalizada esta fase hasta que la Dirección de Seguridad Corporativa dé su visto bueno a la calidad y a la completitud de los entregables de los trabajos que se hayan realizado dentro de esta fase.

Los entregables de esta fase serán:

- i. Las actas de cada una de las entrevistas realizadas a las Unidades Organizativas.
- ii. El informe detallado sobre el estado de la gestión y el nivel de actividad actual de la Agencia en materia de seguridad.

Fase 2 – Diseño y desarrollo del nuevo modelo de gestión de la ciberseguridad para la Agencia Madrid Digital. (Duración estimada: 4 semanas).

Como resultado del análisis de las capacidades de Madrid Digital realizado en la fase anterior, el adjudicatario presentará en esta fase a la Dirección del Proyecto una propuesta de Nuevo Modelo de Gestión de la Ciberseguridad que estará estructurado, según premisa inicial del proyecto, por ámbitos de ciberseguridad, por capacidades de gestión por ámbito y por servicios a prestar en cada capacidad de gestión.

El Nuevo Modelo de Gestión de la Ciberseguridad deberá estar basado en un Marco de Referencia, en un Estándar del mercado o en una Estrategia de Seguridad de amplio reconocimiento en el sector.

La Dirección del Proyecto analizará en esta fase el modelo completo que proponga el adjudicatario y analizará si el detalle presentado se corresponde con el comprometido en la oferta como licitador. Promoverá, para ello, cuantas reuniones de aclaración, definición y profundización sean necesarias.

La estructura del nuevo modelo deberá ser coherente con la estructura organizativa de Madrid Digital. Deberá ser fácilmente interpretable en términos prácticos y directamente asumible, con un nivel de impacto organizativo razonable, por las Unidades Organizativas de la Agencia con competencias en seguridad. El proyecto de mejora funcional que de él se derive deberá ser abordable dentro de un plazo no superior a **cuatro años**.

Se promoverán cuantos workshops o sesiones de trabajo sean necesarias para determinar la información precisa y tomar las decisiones que se requieran para realizar la propuesta del modelo de capacidades de ciberseguridad. Estas actividades deberán ser dirigidas y realizadas por el Jefe de Proyecto.

La Dirección del Proyecto marcará el nivel de detalle a alcanzar en los contenidos de la documentación de esta fase y los criterios de calidad de la misma.

Los entregables de esta fase serán:

- i. La propuesta documentada del Nuevo Modelo de Gestión de la Ciberseguridad para la Agencia Madrid Digital.
- ii. La documentación utilizada en los *workshops*, así como los informes finales sobre las conclusiones y acuerdos alcanzados en los mismos.

Fase 3 - Análisis posicional (análisis GAP). (Duración estimada: 3 semanas).

En esta fase, el adjudicatario elaborará y presentará un **informe sobre el grado de madurez** de la gestión y de los servicios de la Agencia en materia de seguridad. Usará como marco de



referencia el nuevo modelo. El adjudicatario deberá antes proponer a la Dirección del Proyecto una metodología concreta de trabajo, que deberá ser aceptada.

El adjudicatario deberá ponderar la importancia de la prestación de cada servicio de ciberseguridad en función del riesgo que suponga para la Comunidad de Madrid su no disponibilidad o su deficiente implementación. Para ello, la Dirección del Proyecto facilitará al adjudicatario, en su momento, la información disponible sobre los objetivos estratégicos de la Comunidad de Madrid en el ámbito de la ciberseguridad. El adjudicatario desarrollará el análisis GAP en base a dos marcos generales de referencia:

- 1) El *Modelo de Capacidades y de Prestación de Servicios de Ciberseguridad* aprobado en la Fase 2.
- 2) El planteamiento estratégico y los objetivos sobre ciberseguridad que tenga definidos en ese momento la Comunidad de Madrid.

Junto con las conclusiones del análisis GAP, el adjudicatario definirá y documentará el nivel de madurez mínimo que debe ofrecer la Agencia en cada uno de los servicios de ciberseguridad comprendidos en el nuevo modelo. Definirá también para cada servicio el nivel óptimo a alcanzar.

La Dirección del Proyecto marcará el nivel de detalle de los contenidos de la documentación de esta fase y los criterios de calidad de la misma.

El entregable de esta fase será:

- i. El informe sobre el grado de madurez (Análisis posicional o Análisis GAP) de la Agencia Madrid Digital en materia de ciberseguridad.

Fase 4 – Desarrollo de los nuevos servicios. (Duración estimada: 2 semanas).

En el nuevo modelo, dependiendo de cada ámbito (Gobierno, Prevención, Detección Respuesta y recuperación) y de cada capacidad de gestión por ámbito, se definirá un abanico de servicios de ciberseguridad que la Agencia Madrid Digital deberá ser capaz de ofrecer a su propio personal, a sus usuarios y clientes y a los ciudadanos.

Por cada servicio de ciberseguridad se concretará:

- i. En qué situaciones se deberá ofrecer.
- ii. Con qué actividades de la Agencia está relacionado y qué nuevas actividades debe comprender.
- iii. A qué activos afecta.
- iv. Qué mapa de roles y responsabilidades tiene asociado.
- v. Qué Unidad Organizativa de la Agencia debe ser la responsable del servicio, cómo lo debe prestar y quiénes son los destinatarios del mismo.
- vi. En función del mapa de roles y responsabilidades definido, qué otras Unidades Organizativas de la Agencia deben colaborar con la responsable primera y de qué forma.
- vii. Qué medios (tecnologías, personas, procesos, procedimientos) requiere la prestación del servicio.



Se promoverán cuantos workshops o sesiones de trabajo sean necesarias para determinar la información precisa y tomar las decisiones que se requieran para realizar la propuesta de servicios de ciberseguridad. Estas actividades deberá ser dirigida y realizada por el Jefe de Proyecto.

La Dirección del Proyecto comprobará que el nivel de detalle y los contenidos de la documentación que presente el adjudicatario en esta fase se corresponden, como mínimo, a lo comprometido en la oferta, y que dicha documentación cumple con los niveles de calidad pactados.

Los entregables de esta fase serán:

- i. El Plan de servicios de ciberseguridad que deberá ser capaz de ofrecer a la CM la Agencia Madrid Digital.
- ii. La documentación utilizada en los *workshops*, así como los informes finales sobre las conclusiones y acuerdos alcanzados en los mismos.

Fase 5 – Plan de proyectos y presentación de resultados. (Duración estimada: 3 semanas).

El adjudicatario definirá un Plan de Acción que tendrá como objetivo conducir a la Agencia desde la situación actual de gestión a los nuevos niveles de desempeño operativo que el nuevo modelo de prestación de servicios de ciberseguridad haya definido. El Plan de Acción estará constituido por el conjunto de proyectos de transformación de ciberseguridad que la Agencia deberá acometer.

Por cada proyecto se concretará:

- i. La Unidad Organizativa de la Agencia que lo debe liderar.
- ii. Las Unidades Organizativas de la Agencia involucradas, junto a la anterior, en su ejecución y el conjunto de actividades que, concretamente, deberán realizar cada una de ellas.
- iii. Los recursos materiales y humanos necesarios, y su plazo de ejecución.
- iv. El umbral de madurez que la Agencia alcanzaría tras su finalización y en qué ámbito, capacidad de gestión y servicio de ciberseguridad lo alcanzaría.
- v. Por cada proyecto, la relación detallada de las tareas a realizar.
- vi. El coste del mantenimiento del nivel de madurez que se alcance tras la ejecución del proyecto.

Se promoverán cuantos workshops o sesiones de trabajo sean necesarias para determinar la información precisa y tomar las decisiones que se requieran para realizar la propuesta de proyectos e inversiones en ciberseguridad. Estas actividades deberá ser dirigida y realizada por el Jefe de Proyecto.

Se prepararán y realizarán cuantas presentaciones sean necesarias para exponer a la Dirección de Madrid Digital los resultados de los trabajos realizados. Estas actividades deberán ser dirigidas y realizadas por el Jefe de Proyecto.

La Dirección del Proyecto comprobará que el nivel de detalle y los contenidos de la documentación que presente el adjudicatario en esta fase se corresponden, como mínimo, a lo comprometido en la oferta y que dicha documentación cumple con los niveles de calidad pactados.



Los entregables de esta fase serán:

- i. El Plan de Acción de Ciberseguridad para la CM, es decir, la documentación asociada al Plan de proyectos de transformación sobre ciberseguridad que la Agencia madrid Digital deberá acometer.
- ii. La documentación utilizada en los *workshops*, así como los informes finales sobre las conclusiones y acuerdos alcanzados en los mismos.
- iii. La documentación empleada para las presentaciones a la Dirección de MadridDigital.

CLÁUSULA 5.- EQUIPO PRESTADOR DEL SERVICIO

Para la prestación de los trabajos objeto del contrato, el adjudicatario pondrá a disposición de Madrid Digital un equipo con la cualificación y el perfil técnico mínimos, que a continuación se detallan:

— Requisitos en cuanto al **A LOS PERFILES Y CATEGORÍA PROFESIONAL MÍNIMA** exigida al personal prestador del servicio:

- Consultor estratégico, que actuará como Jefe de Proyecto.
- Analista de Seguridad expertos en gobierno de la seguridad TIC).

— Requisitos en cuanto a **TITULACIÓN MÍNIMA** exigida a cada uno de los miembros del equipo prestador del servicio:

- Titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente.

— Requisitos en cuanto a **FORMACIÓN MÍNIMA** exigida a cada uno de los miembros del equipo prestador del servicio:

- Disponer de, al menos, una acreditación de **ISACA: Information Systems Audit and Control Association** (Asociación de Auditoría y Control de Sistemas de Información).

— Requisitos en cuanto **ACTIVIDAD PROFESIONAL MÍNIMA** exigida a cada uno de los miembros del equipo prestador del servicio:

Para el Consultor estratégico:

- Haber participado, durante al menos **siete años**, como Consultor en proyectos de asesoría y consultoría estratégica de seguridad de la información y en la realización de Planes Directores de Seguridad Corporativa.

Para el Analista de Seguridad:

- Haber participado, durante al menos **cinco años**, como Consultor en proyectos de asesoría y consultoría estratégica de seguridad de la información y en la realización de Planes Directores de Seguridad Corporativa.

Al efecto, el licitador propuesto como adjudicatario, con carácter previo a la formalización del contrato, deberá aportar el *currículum vitae* de las personas asignadas a la ejecución del



contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).

CLÁUSULA 6.- VERIFICACIÓN DE LA CAPACIDAD DE LOS COMPONENTES DEL EQUIPO ADSCRITO A LA EJECUCIÓN DEL CONTRATO Y SUSTITUCIÓN DE LOS COMPONENTES DE DICHO EQUIPO

6.1. Condicionantes del equipo de trabajo:

El contratista responderá siempre de la adecuación del personal encargado de la realización de los servicios objeto del contrato, que responderá siempre a los *requisitos mínimos* que en el presente Pliego de Cláusulas Técnicas se señalan.

La falsedad en el nivel de conocimientos técnicos del equipo adscrito al servicio, facultará a esta Agencia para instar la **resolución** del contrato.

6.2. Constitución inicial del equipo de trabajo:

El equipo humano que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por todos y cada uno de las personas desinadas por el licitador propuesto como adjudicatario y, en todo caso, habiéndose verificado previamente, por parte del *Responsable del Contrato* de Madrid Digital, que cada *currículum vitae* cumple los requisitos mínimos establecidos en este pliego.

Si en la fecha de inicio de la ejecución, los trabajos objeto del contrato no hubieran comenzado y no se pudiera contar en tal fecha con la disponibilidad del equipo necesario para la atención de los mismos, facultará a esta Agencia para instar la **resolución** del contrato.

6.3. Modificaciones en la composición del equipo de trabajo:

La valoración final de la calidad de los trabajos desarrollados por las personas adscritas a la ejecución del contrato corresponde al *Responsable del Contrato*, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual categoría, si existen razones justificadas que lo aconsejen.

Asimismo, Madrid Digital podrá exigir la incorporación de más miembros al equipo de trabajo o refuerzos cuando sean necesarios para garantizar el cumplimiento de cada uno de los plazos comprometidos por el adjudicatario en su *Propuesta Técnica*, de tal forma que se asegure la finalización de las fases en tiempo y forma.

Si fuera la firma adjudicataria la que propusiera el cambio de una de las personas del equipo de trabajo, se deberá solicitar por escrito con quince días de antelación, exponiendo las razones que obligan a la propuesta. En su caso, el cambio deberá ser aprobado por el *Responsable del Contrato*.



CLÁUSULA 7.- CONDICIONES ADICIONALES A CUMPLIR

7.1. Disponibilidad de medios y verificación de la capacidad

El adjudicatario deberá contar con los medios propios, personales y materiales, necesarios de cara al soporte técnico que pueda necesitar, para llevar a cabo con éxito todos los servicios objeto del contrato, teniendo en cuenta que, en todo caso, el equipo prestador del servicio se ubicará en las instalaciones que Madrid Digital determine, dentro de la franja horaria de permanencia que la Dirección de Seguridad Corporativa establezca para el proyecto.

Los empleados de la empresa contratista, que ejecuten por cuenta de ésta trabajos directamente relacionados con el objeto del contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por la propia empresa contratista. No obstante, si fuese necesario por razones operativas asociadas a la naturaleza del servicio a prestar, Madrid Digital proporcionaría a los miembros del equipo adscrito a la ejecución del servicio los medios que estime oportunos para la ejecución de los trabajos y obligaciones demandadas.

La dotación de dichos medios tiene naturaleza transitoria, ya que se utilizarán únicamente durante la ejecución del contrato, además su uso estará limitado exclusivamente al desarrollo de los trabajos que constituyen el objeto del contrato. En todo caso, Madrid Digital adoptará las medidas necesarias para que estas herramientas tengan una identificación diferenciada respecto de las asignadas al personal al servicio de Madrid Digital.

En el caso de que, por razones ajenas a Madrid Digital, los trabajos contratados puedan implicar para el contratista la decisión de ejecución de los mismos en régimen de turnos, en sábados o festivos, o en horario nocturno, esta Agencia no aceptará sobrecostes adicionales por estas circunstancias, que deberán ser asumidos siempre por el contratista.

7.2. Certificación de un Sistema de Gestión de Seguridad de la Información

Las empresas licitadoras deberán aportar certificación vigente acreditativa de disponer y mantener operativo un *Sistema de Gestión de Seguridad de la Información*, de acuerdo a la norma internacional ISO 27001, emitido por una entidad acreditada por ENAC o equivalente.

7.3. Responsable del Servicio

El contratista designará a un **Responsable del Servicio**, que deberá estar expresamente identificado, que será el responsable del mismo ante Madrid Digital.

Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la Dirección de Madrid Digital designe a los efectos que se señalan en *la Cláusula 19 del Pliego de Cláusulas Jurídicas*.

El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que Madrid Digital determine, asistirá a las reuniones de seguimiento del proyecto, informará sobre la planificación de trabajos, el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas. En particular, este responsable será el interlocutor único entre el adjudicatario y Madrid Digital. Coordinará todo el proyecto y será el responsable, en último término, de la buena marcha de los trabajos. Entre sus **tareas** principales cabe destacar las siguientes:



- Coordinar la ejecución de los trabajos.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Supervisar y controlar la calidad de las actividades desarrolladas por su equipo.
- Hacer entrega a Madrid Digital de los documentos desarrollados por su equipo.

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

CLÁUSULA 8.- SEGUIMIENTO Y CONTROL DEL CONTRATO

El seguimiento y control del contrato se efectuará sobre las siguientes bases:

Seguimiento continuo de la evolución de los trabajos entre el *Responsable del Servicio* por parte del adjudicatario y el *Responsable del Contrato* que Madrid Digital designe.

Madrid Digital determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control de los trabajos.

CLÁUSULA 9.- PLAZO DE GARANTÍA

Se establece un plazo de garantía del contrato de **4 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 adjudicatario responderá de la correcta ejecución de los trabajos contratados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de Madrid Digital 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 trabajos ejecutados.

CLÁUSULA 10.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Normativa aplicable.

1. 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).*
 - Y las 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.

2. 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*):

2.1 En la fase de diseño funcional del sistema de referencia se realizará un **estudio previo de datos de carácter personal** a tratar, su naturaleza y las medidas de seguridad que requieran de conformidad con la naturaleza de los datos y los requerimientos del *RD 1720/2007*. Si procede igualmente se propondrá la correspondiente creación e inscripción en la Agencia Española de Protección de Datos.

2.2 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 Madrid Digital, y en concreto:

2.2.1 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.

2.2.2 Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El contratista se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

2.2.3 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 Madrid Digital. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por Madrid Digital. 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.

2.2.4 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.

2.2.5 Solo con el consentimiento expreso y escrito de Madrid Digital, 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.

2.2.6 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.

- 2.2.7 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.
 - 2.2.8 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.
 - 2.2.9 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
- 2.3** 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:
- 2.3.1 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.
 - 2.3.2 Exclusivamente el personal autorizado por Madrid Digital podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
 - 2.3.3 Será necesaria la autorización de Madrid Digital para la ejecución de los procedimientos de recuperación de los datos.
- 2.4** 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:
- 2.4.1 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 Madrid Digital.

- 2.4.2 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.
- 2.4.3 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.
- 2.4.5 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.
- 2.4.6 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.

Personal prestador del servicio.

- 3. Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal firmarán un documento por el que quedarán obligados al **secreto profesional** respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar la relación contractual. Así como a la renuncia expresa de los derechos de **propiedad intelectual** que les pudiera corresponder y compromiso del cumplimiento de las obligaciones de protección de datos de carácter personal.

El contratista nombrará de dentro del equipo prestador del servicio a un miembro como **Responsable de Seguridad**, que se encargará de la puesta en práctica y de la inspección de las medidas de seguridad, informando de su nombre y puesto a la Agencia.

El contratista se compromete a **formar e informar a su personal** en las obligaciones que de tales normas dimanen, para lo cual programará las acciones formativas necesarias.

El personal prestador del objeto del contrato tendrá **acceso autorizado** únicamente a aquellos datos y recursos que precisen para el **desarrollo de sus funciones**.

Cesión o comunicación de datos a terceros.

- 4. 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 Madrid Digital, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
- 5. 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 Madrid Digital, el equipo prestador del servicio procederá a destruir o a devolver a Madrid Digital 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.

6. 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*, Madrid Digital, 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.

- 8 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 para Madrid Digital, inscrito en el Registro General de Ficheros de Datos Personales de la Agencia Española de Protección de Datos, y no podrán ser cedidos salvo por los supuestos previstos en la Ley. El Órgano responsable del fichero es el *Consejero-Delegado de Madrid Digital*, 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*.

CLÁUSULA 11.- SEGURIDAD DE LA INFORMACIÓN TRATADA

La empresa adjudicataria, así como todos los componentes del equipo adscrito a la ejecución de los trabajos objeto del presente contrato, asumen las siguientes obligaciones:



11.1. Sigilo y confidencialidad de la información tratada

Cada uno de los componentes del Equipo prestador del servicio se compromete a proteger la confidencialidad de cualquier información tratada como consecuencia de la ejecución de los trabajos derivados del contrato.

Todos los componentes del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información dimanante de la ejecución del contrato.

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, ceder o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución.

Esta obligación no se limita al tiempo de ejecución del presente contrato, 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 Madrid Digital, la Comunidad de Madrid o cualquier tercero que tenga relaciones contractuales con la misma, en relación con el objeto del presente contrato, será considerada como «Información Confidencial», incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

El Equipo prestador del servicio deberá:

- 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 prestador del servicio.
- Utilizar o transmitir la Información Confidencial exclusivamente para los fines del contrato.
- No realizar copia de la Información Confidencial sin el previo consentimiento escrito de Madrid Digital, excepto aquellas copias que sean necesitadas por el Equipo prestador del servicio.
- Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del Contrato.

Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del presente Contrato o a su contenido, deberá ser previamente aprobada por escrito por Madrid Digital.

El Equipo prestador del servicio procederá a destruir o a devolver a Madrid Digital toda la Información Confidencial a la finalización del contrato, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida. La destrucción o devolución de la Información Confidencial 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.

11.2. Modificaciones en la composición del Equipo prestador del servicio

En el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en el presente documento.



A tal efecto, el firmante del presente documento, se compromete a formar e informar al nuevo personal de tales obligaciones, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.

CLÁUSULA 12.- 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 Madrid Digital, 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 de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de Madrid Digital.

CLÁUSULA 13.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE MADRID DIGITAL

El contratista no adquiere ningún derecho sobre el hardware (material), software e infraestructuras propiedad de Madrid Digital, 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, no pudiendo transmitir dicho conocimiento, sin el consentimiento expreso y por escrito de Madrid Digital.

CLÁUSULA 14.- CALIDAD

Durante el periodo de ejecución del contrato, el adjudicatario propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada.

No obstante, Madrid Digital podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, la Agencia podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

CLÁUSULA 15.- CONTENIDO MÍNIMO DE LAS OFERTAS

En el presente apartado se describe la estructura según la cual deberán elaborarse las ofertas presentadas por cada uno de los licitadores. Para la elaboración de la citada propuesta los licitadores deberán basarse en los requerimientos recogidos en este Pliego. La oferta debe incorporar la totalidad de los trabajos solicitados en el Pliego, de manera que no se admitirán ofertas parciales por actividad.

Con carácter obligatorio, la memoria deberá presentarse en papel y en soporte electrónico, compatible con las herramientas instaladas en Madrid Digital (MS Word 2007, Adobe Acrobat Reader 8, MS Explorer 7).

Los licitadores deberán evitar descripciones genéricas o excesivamente prolijas que puedan perjudicar la comprensión de la oferta técnica directamente diseñada y ofrecida a Madrid Digital. El licitador deberá ajustarse especialmente a lo indicado en este punto, y circunscribir su propuesta exclusivamente a lo demandado en el pliego.



La **estructura** según la cual deberán elaborarse las ofertas a presentar por los licitadores es la siguiente:

1. Planificación, metodología y alcance del proyecto

- Planificación detallada del proyecto, con especificación de fases y actividades asociadas, incluyendo dedicación esperada de Madrid Digital.
- Descripción detallada de la metodología de trabajo y de las actividades para desarrollar las tareas objeto del servicio, con la garantía de calidad requerida.

Se prestará una especial atención a aquellos aspectos de la propuesta para los que el presente pliego requiere la máxima precisión y el mayor detalle posible de desarrollo.

- Descripción detallada de la solución propuesta para el servicio de análisis y medición integral de cumplimiento así como del sistema aportado para la obtención de la información respecto del análisis y medición del cumplimiento de las distintas regulaciones normativas en materia de seguridad.
- Descripción de la documentación y de los entregables comprometidos para cada una de las líneas de servicio definidas.

El criterio de valoración vinculado a esta parte de la oferta es el : *Subcriterio 2.1*

2. Seguimiento y control del servicio

Descripción del modelo de seguimiento del servicio:

- Propuesta detallada de cada uno de los Informes a elaborar para el seguimiento de los periodos definidos.
- Métricas adicionales, así como cualquier otro aspecto de valor para el seguimiento y control del servicio que el licitador comprometa, que permita afianzar y mejorar el modelo de servicio de Madrid Digital.

El criterio de valoración vinculado a esta parte de la oferta es el : *Subcriterio 2.1*

3. Organización de los equipos de trabajo propuestos

Propuesta y descripción de la estructura de los equipos de trabajo, especialmente en lo que se refiere a:

- Composición, organización y dedicación del equipo de trabajo propuesto, para cada uno de los trabajos y de las fases correspondientes: Debe quedar claro el número total de recursos que van a estar involucrados en los servicios, los perfiles que tienen, las fases en las que participarán y las horas de dedicación de cada recurso en cada una de las fases.
- Asegurar la estabilidad del equipo.
- Comprometer la implicación de los equipos de trabajo en situaciones de crisis, en las que prima la continuidad del servicio objeto de contratación.
- Propuestas de valor cuya aplicación sea factible, de manera que permitan a Madrid Digital obtener la flexibilidad en la gestión de las capacidades necesaria ante picos de trabajo.

El criterio de valoración vinculado a esta parte de la oferta es el : *Subcriterio 2.2*



4. **Anexos: Detalle y ejemplos de servicios y de proyectos**

Servicios de ciberseguridad:

Se aportarán **cuatro ejemplos completos y detallados de servicios de ciberseguridad**, uno por cada ámbito general (Gobierno, Prevención, Detección, Respuesta y recuperación), con el desarrollo completo de todos sus elementos, tal y como lo presentará finalmente, si resultara adjudicatario, para todos y cada uno de los servicios del modelo final de ciberseguridad. Este detalle incluirá:

- La definición de la estructura organizativa necesaria para la prestación de cada servicio.
- El desarrollo y concreción de los componentes y las actividades de cada servicio.
- La descripción de los recursos necesarios para la implementación de cada servicio.

El criterio de valoración vinculado a esta parte de la oferta es el : Subcriterio 2.3

Proyectos de mejora:

Se aportarán **cuatro ejemplos completos y detallados de proyectos de mejora de servicios**, uno por cada ámbito general (Gobierno, Prevención, Detección, Respuesta y recuperación) con el desarrollo completo de todos sus elementos, tal y como lo presentará finalmente, si resultara adjudicatario, para todos y cada uno de los proyectos del plan de mejora definitivo. Este detalle incluirá:

- La definición de la estructura organizativa necesaria para la ejecución de cada proyecto.
- El desarrollo y concreción de los componentes y las actividades de cada proyecto.
- La descripción de los recursos necesarios para la ejecución del proyecto.

El criterio de valoración vinculado a esta parte de la oferta es el : Subcriterio 2.4

CLÁUSULA 16.- PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **DIECISEIS SEMANAS**, a contar desde el día siguiente a la formalización del contrato y con los siguientes plazos parciales:

- Fase 1 - Planificación preliminar de los trabajos y análisis de la actividad de la Agencia en materia de seguridad. (Duración estimada: 4 semanas)
- Fase 2 - Diseño y desarrollo del nuevo modelo de gestión de la ciberseguridad para la Agencia. (Duración estimada: 4 semanas)
- Fase 3 - Análisis posicional (análisis GAP). (Duración estimada: 3 semanas)
- Fase 4 - Desarrollo de los nuevos servicios. (Duración estimada: 2 semanas)
- Fase 5 - Plan de Proyectos. (Duración estimada: 3 semanas).

Si en la fecha de inicio de la ejecución, los trabajos objeto del contrato no hubieran comenzado, y no se pudiera contar en tal fecha con la disponibilidad del equipo necesario para la ejecución de los mismos, Madrid Digital quedará facultada para instar la **resolución** del contrato.



CLÁUSULA 17.- 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 podrán dirigirse a:

***Dirección de Seguridad Corporativa
Agencia para la Administración Digital de la Comunidad de Madrid***

C/ Embajadores, 181

28045 Madrid

Tel.: 91 580 50 00

Horario de consultas: de 9 a 14 horas, de lunes a viernes

*ELABORADO Y PROPUESTO POR:
El Director de Seguridad Corporativa*

Fdo.: Fernando Ledrado Gómez

*APROBADO POR:
El Consejero Delegado de la Agencia para la Administración
Digital de la C.M.*

Fdo.: Blas Labrador Román

