

Pliego de Prescripciones Técnicas que han de regir el contrato de servicios denominado:  
**“OFICINA DE GOBIERNO DE LA SEGURIDAD DE MADRID DIGITAL”**  
a adjudicar mediante **procedimiento** abierto con pluralidad de criterios



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv)  
mediante el siguiente código seguro de verificación: **1019629385769945216829**

## INDICE

CLÁUSULA 1.-	INTRODUCCIÓN.....	5
CLÁUSULA 2.-	OBJETO Y ALCANCE.....	5
CLÁUSULA 3.-	CONSIDERACIONES GENERALES.....	5
CLÁUSULA 4.-	CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR POR LA OGS .....	6
4.1	Ámbito: GOBIERNO DE LA SEGURIDAD .....	7
4.1.1	Capacidad: GOBIERNO Y GESTIÓN DEL RIESGO .....	7
4.1.1.1	Gestión de activos .....	7
4.1.1.2	Catálogo de amenazas .....	7
4.1.1.3	Análisis de riesgos .....	7
4.1.1.4	Análisis de auditorías y cumplimiento .....	7
4.1.1.5	Seguridad en la relación con proveedores.....	8
4.1.2	Capacidad: GESTIÓN, REPORTE Y CONTROL .....	8
4.1.2.1	Reporte a Comités y Organismos .....	8
4.1.2.2	Comunicación.....	9
4.1.2.3	Herramientas de control y seguimiento .....	9
4.1.2.4	Elaboración de planes de acción y seguimiento de despliegues.....	9
4.1.3	Capacidad: CUMPLIMIENTO NORMATIVO .....	10
4.1.3.1	Identificación de la regulación aplicable.....	10
4.1.3.2	Definición de la Política de Seguridad .....	10
4.1.3.3	Definición de la normativa de seguridad .....	10
4.1.3.4	Definición de planes de formación y concienciación .....	10
4.2	Ámbito: PREVENCIÓN .....	11
4.2.1	Capacidad: PROCEDIMIENTOS Y PROCESOS DE PROTECCIÓN .....	11
4.2.1.1	Asesoramiento en seguridad .....	11
4.2.1.2	Tratamiento de excepciones de seguridad.....	11
4.2.2	Capacidad: PROTECCIÓN DE LA INFRAESTRUCTURA.....	11
4.2.2.1	Protección ambiental y áreas seguras .....	11
4.2.3	Capacidad: PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN .....	12
4.2.3.1	Requisitos de seguridad en sistemas de información .....	12
4.2.4	Capacidad: GESTIÓN DE IDENTIDADES Y ACCESOS .....	12
4.2.4.1	Seguridad en la identidad digital.....	12
4.2.4.2	Seguridad en el acceso físico.....	12
4.2.5	Capacidad: FORMACIÓN Y CONCIENCIACIÓN .....	12
4.2.5.1	Formación y concienciación en seguridad y prevención de riesgos laborales para la Dirección .....	13
4.2.5.2	Formación y concienciación en seguridad para el personal.....	13
4.2.5.3	Ciudadanos y campañas de comunicación.....	13
4.2.6	Capacidad: SEGURIDAD DE LOS RRHH.....	13
4.2.6.1	Seguridad en relaciones laborales.....	13



4.2.6.2	Prevención, gestión de riesgos e incidentes laborales.....	14
4.2.6.3	Seguridad física de las personas .....	14
4.3	Ámbito: DETECCIÓN .....	14
4.3.1	Capacidad: PROCEDIMIENTOS Y PROCESOS DE DETECCIÓN .....	14
4.3.1.1	Relación con agentes externos .....	14
4.3.1.2	Colaboración con Fuerzas y Cuerpos de Seguridad del Estado .....	15
4.4	Ámbito: RESPUESTA Y RECUPERACIÓN.....	15
4.4.1	Capacidad: RESPUESTA ANTE INCIDENTES .....	15
4.4.1.1	Análisis y peritaje forense.....	15
4.4.2	Capacidad: ASEGURAMIENTO DE LA CONTINUIDAD .....	15
4.4.2.1	Definición y mantenimiento de Planes de Continuidad.....	15
4.4.2.2	Gestión de crisis .....	16
4.4.2.3	Simulacros de los planes de continuidad.....	16
4.4.2.4	Aprendizaje de los simulacros de los planes de continuidad .....	16
4.5	EQUIPO DE TRABAJO .....	16
4.5.1	Equipo Base: Líneas de actuación y actividades a desarrollar. ....	20
4.5.2	Equipo Proyecto: Líneas de actuación y actividades a desarrollar. ....	24
4.6	HORARIO Y UBICACIÓN .....	26
4.7	TECNOLOGÍAS Y HERRAMIENTAS .....	27
CLÁUSULA 5.-	MODELO DE GESTIÓN .....	28
5.1	DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS .....	28
5.1.1	Comité de seguimiento del contrato (CSC). ....	28
5.1.2	Comité Técnico y Operativo (CTO). ....	29
5.2	CONDICIONES GENERALES DE LOS RECURSOS DEL ADJUDICATARIO .....	30
5.2.1	Condiciones de estabilidad del equipo de trabajo .....	31
5.2.2	Modificaciones en la composición del equipo de trabajo a petición de la Agencia .....	31
5.3	SEGUIMIENTO Y MEJORA CONTINUA DEL SERVICIO.....	31
5.4	FACTURACIÓN DE LOS SERVICIOS.....	32
CLÁUSULA 6.-	CONTENIDO DE LAS OFERTAS.....	32
6.1	CONTENIDO DE LAS OFERTAS .....	33
6.1.1	Índice.....	33
6.1.2	Solución técnica propuesta para los servicios requeridos.....	33
6.1.2.1	Planificación, alcance y descripción del proyecto. ....	33
6.1.2.2	Plan de implantación de los servicios. ....	33
6.1.2.3	Plan de operación y devolución de los servicios. ....	34
6.1.2.4	Organización del equipo de proyecto. ....	34
6.1.2.5	Plan de Calidad .....	34
6.1.2.6	Plan de capacitación y formación .....	34
CLÁUSULA 7.-	GESTIÓN DE LA SEGURIDAD .....	34
7.1	Normativa.....	34



7.2	Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento .....	35
7.3	Obligaciones de la Agencia Madrid Digital para la prestación del servicio .....	38
7.4	Sub-encargos de tratamiento asociados a Subcontrataciones .....	38
7.5	Tratamiento de datos personales .....	38
7.6	Deber de Información.....	38
Seguridad en la utilización de medios electrónicos.....		39
7.7	Normativa .....	39
7.8	Conformidad con el Esquema Nacional de Seguridad.....	39
Medidas de Seguridad .....		39
7.9	Documentación de seguridad .....	39
7.10	Confidencialidad y deber de secreto .....	40
CLÁUSULA 8.-	PROPIEDAD DE LOS TRABAJOS.....	40
CLÁUSULA 9.-	DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS .....	40
CLÁUSULA 10.-	CALIDAD DEL SERVICIO .....	40
CLÁUSULA 11.-	PLAZO, DURACIÓN Y ETAPAS DE PRESTACIÓN DE LOS SERVICIOS .....	41
CLÁUSULA 12.-	GARANTÍA DE LOS TRABAJOS.....	42
CLÁUSULA 13.-	CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS.....	42
ANEXO I. MODELO DE CURRÍCULUM .....		43
ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES .....		44



## CLÁUSULA 1.- INTRODUCCIÓN

La **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante Madrid Digital ó MD), según se establece en la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas, modificada parcialmente por la Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015), 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 la seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad (Artículo 10, Tres ).

Madrid Digital ha elaborado un plan estratégico (en adelante PEMD) que recoge los ejes estratégicos de acción y las líneas de actuación que Madrid Digital debe impulsar con el objetivo de ayudar a alcanzar los objetivos planteados en el plan estratégico de innovación y modernización de la gestión pública de la Comunidad de Madrid.

En particular, el eje estratégico "Tecnología e innovación para la transformación digital" incluye la línea de actuación de ciberseguridad, que a su vez determina la ejecución de los siguientes programas:

- Estrategia corporativa de seguridad de los servicios digitales
- Garantizar la seguridad de los servicios, los datos y su disponibilidad
- Fortalecer las capacidades de prevención, detección y respuesta ante ciberataques

En el marco de dichos programas, Madrid Digital ha finalizado recientemente la definición del modelo funcional y organizativo de ciberseguridad de Madrid Digital. Como resultado de este modelo, entre otros, se ha determinado las capacidades de ciberseguridad que Madrid Digital debe asumir y se ha concretado, en cada caso, las funciones y servicios que deben prestarse, tanto en el ámbito de la estrategia y dirección, en la de gestión y control y en la de operación de la ciberseguridad.

## CLÁUSULA 2.- OBJETO Y ALCANCE

El presente *Pliego de Prescripciones Técnicas* (en adelante PPT) incluye la contratación de los servicios de seguridad de una *Oficina de Gobierno de Seguridad* (en adelante OGS) que son necesarios para abordar y ejecutar los trabajos destinados a impulsar y adquirir determinadas capacidades, funciones y servicios de ciberseguridad que se detallan en el modelo funcional y organizativo de ciberseguridad de Madrid Digital.

## CLÁUSULA 3.- CONSIDERACIONES GENERALES

Con carácter obligatorio, los adjudicatarios se responsabilizarán durante el periodo de ejecución del contrato de la correcta operación, mantenimiento y actualización de los servicios requeridos, así como de los equipamientos, soluciones y herramientas que propongan para la prestación de los mismos.

Estarán obligados a conocer y observar la normativa interna aplicable en Madrid Digital, así como a incorporarla y tenerla en cuenta durante la ejecución del contrato. Ejemplos de este punto son políticas de control de acceso y gestión de recursos vigentes, normativas de seguridad aplicables, de instalación, de gestión patrimonial de equipamientos, procedimientos operativos relacionados con la gestión de TIC, etc.

La prestación de los servicios objeto de este Pliego de Prescripciones Técnicas conllevará el cumplimiento de unos niveles de servicio acordados o comprometidos (ANS – Acuerdo de Nivel de Servicio), así como la definición de una política de penalizaciones ante incumplimientos, que los adjudicatarios estarán obligados a aceptar. Los niveles de servicio definidos se recogen en el **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**.

El objeto de la presente contratación de los servicios de seguridad de una Oficina de Gobierno de Seguridad (OGS) que son necesarios para abordar y ejecutar los trabajos destinados a impulsar y adquirir determinadas capacidades, funciones y servicios de ciberseguridad que se detallan en el modelo funcional y organizativo de ciberseguridad de Madrid Digital.

Estas funciones de la OGS implican necesariamente la vigilancia, supervisión y control de la ejecución de cualesquiera servicios sean llevados a cabo por el Centro de Operaciones de Seguridad de Ciberseguridad de la Agencia para la Administración Digital de la Comunidad a contratar bajo el título "DISEÑO,



IMPLEMENTACIÓN Y SUPERVISIÓN DE SERVICIOS DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID” con ECON/000079/2018, y por tanto se incurre en las condiciones especiales de compatibilidad establecidas en el artículo 70 de la ley 9/2017, implicando ello que **no podrá adjudicarse el contrato** titulado “OFICINA DE GOBIERNO DE LA SEGURIDAD DE MADRID DIGITAL (OGS)” ECON 000141/2018 **a las mismas empresas adjudicatarias** de los correspondientes dos lotes previstos en el contrato titulado “DISEÑO, IMPLEMENTACIÓN Y SUPERVISIÓN DE SERVICIOS DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID” con ECON/000079/2018, ni a las empresas a estas vinculadas.

<b>CLÁUSULA 4.-</b>	<b>CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR POR LA OGS</b>
---------------------	--

La **Oficina de Gobierno de la Seguridad (OGS)** dispondrá de manera autosuficiente de los recursos técnicos, humanos, logísticos y materiales necesarios para proporcionar asistencia y soporte a Madrid Digital (MD) en todos y cada uno de los ámbitos, funciones, capacidades y servicios que se enumeran en este Pliego.

Madrid Digital estima que para dotar la OGS son necesarios, como mínimo, los perfiles profesionales y los efectivos humanos que se describen en el apartado **4.5 EQUIPO DE TRABAJO** de este pliego. El adjudicatario deberá incorporar al servicio, de forma permanente u ocasional, los efectivos y los perfiles profesionales adicionales que sean necesarios para dar cobertura a las funciones y servicios a prestar por la Oficina, descritos en este apartado. Estas dotaciones adicionales, aportadas presencialmente o desde las dependencias del adjudicatario, no supondrán nunca un sobrecoste para MD.

El adjudicatario aportará, especialmente, personal de apoyo y soporte siempre que sea preciso cumplir objetivos de calidad y plazos de entrega comprometidos por la Dirección de Seguridad Corporativa con Madrid Digital o desde Madrid Digital hacia la Comunidad de Madrid, cuando estos servicios o proyectos tengan relación con la actividad de la Oficina. Igualmente que en el párrafo anterior, estos recursos, en caso de ser necesarios, no supondrán sobrecoste alguno para MD. El responsable de Gobierno, Riesgo y Cumplimiento de MD comunicará oportunamente a la OGS dichos plazos y objetivos así como cualquier otro condicionante o aspecto del servicio que deba ser tenida en cuenta obligatoriamente por la OGS.

El incumplimiento de estos requisitos del pliego será motivo de penalización. (Ver **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**)

El adjudicatario aportará por su cuenta al contrato las herramientas necesarias para la prestación del servicio (Apartado **4.7 TECNOLOGÍAS Y HERRAMIENTAS**).

La OGS empleará únicamente formatos y soportes lógicos o físicos para la gestión de la información compatibles con los homologados por MD.

La cualificación profesional del equipo humano de la OGS y su actividad diaria o por proyectos - tendrá relación directa con las siguientes materias del ámbito de la seguridad legal y de las tecnologías de la información y las comunicaciones:

- Análisis de vulnerabilidades y amenazas de los activos TIC
- Inventariado, organización y gestión de activos TIC
- Metodologías de análisis de riesgos
- Gestión del riesgo y su mitigación
- Despliegue de planes, programas y herramientas de control
- Administración y operación de herramientas y plataformas de gestión de la seguridad
- Generación de normativa de seguridad
- Análisis de normativa, soporte legal, a MD y a la Comunidad de Madrid
- Análisis, investigación y peritaje forense
- Administración electrónica (ámbitos tecnológico y normativo, nacional y de la UE)
- Legislación sobre seguridad, protección de datos, identificación electrónica y servicios de confianza en el ámbito nacional y de la UE
- Establecimiento de modelos y requisitos de seguridad para la identidad digital
- Gestión de certificados electrónicos y normativa sobre firma electrónica



- Planes de continuidad de negocio
- Planes de recuperación frente a desastres
- Gestión documental de la seguridad
- Diseño y ejecución de planes de concienciación y formación
- Seguridad en código software
- Buenas prácticas de desarrollo seguro
- Tratamiento y respuesta frente a incidentes de seguridad
- Asistencia forense y pericial a MD en juicios

La actividad de la **Oficina de Gobierno de la Seguridad (OGS)** se organizará en cuatro **ámbitos** principales: **1-Gobierno, 2-Prevención, 3- Detección y 4-Recuperación y Respuesta**, y dentro de cada uno de ellos se definen, en los siguientes apartados, las **capacidades** a desarrollar, las **funciones** a desempeñar y los **servicios** a prestar bajo las directrices de MD.

La **OGS** llevará acabo, bajo la dirección de MD, las siguientes actividades:

#### **4.1 Ámbito: GOBIERNO DE LA SEGURIDAD**

##### **4.1.1 Capacidad: GOBIERNO Y GESTIÓN DEL RIESGO**

###### **Servicios a prestar:**

###### **4.1.1.1 Gestión de activos**

La OGS establecerá una metodología para la gestión de los activos que contemple la identificación, inventariado, clasificación y sus diferentes tipologías. Establecerá también una metodología para su valoración y los criterios para su actualización periódica, todo ello enfocado a la aplicación de los procesos necesarios para el posterior análisis de riesgos.

Se realizará un seguimiento del proceso de inventariado, que asegurará que se realiza de acuerdo a la metodología previamente definida. Se verificará que la clasificación y valoración son coherentes entre los diferentes tipos de activos, de modo que las dependencias entre los mismos estén registradas adecuadamente y los criterios de valoración y priorización cumplen con la estrategia de ciberseguridad de la Agencia.

Se asegurará que se define la propiedad de cada activo así como la responsabilidad sobre su clasificación y la aplicación de los controles necesarios en cada caso.

###### **4.1.1.2 Catálogo de amenazas**

La OGS establecerá una metodología para la gestión del catálogo de amenazas que contemple tanto el mecanismo de identificación como su inventariado. Establecerá además un criterio para la valoración de las amenazas y su actualización, de modo que sirvan como base permanente del consiguiente análisis de riesgos.

La identificación, clasificación y valoración de las amenazas registradas en el catálogo sustentará el modelo de gobierno y la gestión del riesgo.

###### **4.1.1.3 Análisis de riesgos**

La OGS establecerá una metodología que satisfaga los requisitos legales y de normativa interna para la valoración y determinación del riesgo de los activos de la Agencia. Se definirán los criterios para el reporte periódico de los niveles de riesgo así como el mecanismo de notificación en caso de superarse el apetito de riesgo.

Será objeto de este servicio la realización de todas las actividades necesarias para poder determinar el riesgo final de cualquier activo de la Agencia. Entre otras, será necesario realizar las siguientes:





- Identificar requisitos de seguridad y su aplicabilidad para incorporarlos en los activos de la Agencia para eliminar o minimizar la probabilidad de explotación de las posibles vulnerabilidades.
- Identificar criterios de valoración homogéneos que faciliten a los responsables la categorización de sistemas de información según el Esquema Nacional de Seguridad.
- Dar soporte a las Unidades de la Agencia en la especificación de los requisitos anteriores y en la implantación de los mismos durante las fases de diseño y puesta en marcha de servicios y en la valoración y categorización de sistemas de información.
- Verificar la implantación real de aquellos requisitos de seguridad que se hayan identificado como aplicables en la fase de diseño de un servicio.
- Determinar la madurez de los requisitos de seguridad implantados conforme a la metodología definida en gestión de riesgos, evidenciando y documentando los resultados en informes y aplicaciones corporativas.
- Dar soporte a las Unidades de la Agencia que sean responsables de activos en la asignación del impacto de forma que se determine el valor del daño que produciría la degradación o pérdida de funcionalidad del activo al materializarse una amenaza por una inadecuada o inexistente implantación de un requisito de seguridad.

El análisis de riesgo se realizará de forma continua, con el objetivo de determinar los niveles de riesgo existentes en cada momento, de acuerdo con los criterios de valoración y la metodología definidos.

#### **4.1.1.4 Análisis de auditorías y cumplimiento**

La OGS analizará los resultados de todas aquellas auditorías o revisiones de cumplimiento que se lleven a cabo. Se agregarán los resultados al análisis de riesgos como parte del plan de mejora del tratamiento de riesgos.

Las conclusiones y hallazgos relevantes derivados del plan de auditorías, proporcionarán la base para el aseguramiento del nivel de riesgo por debajo de los umbrales definidos.

#### **4.1.1.5 Seguridad en la relación con proveedores**

La OGS analizará y gestionará el nivel riesgo en las relaciones con proveedores, dado que la transferencia de actividad operativa a éstos no transfiere las responsabilidades de MD en materia de gestión de activos o análisis de riesgos.

El riesgo inherente a la relación con proveedores podrá tratarse de diferentes modos (existencia de políticas, normativas, acuerdos de nivel de servicios (ANS), ciberseguros...etc.). Estos modos de tratamiento deberán ser valorados dentro del análisis de riesgos global. La OGS desarrollará las cláusulas de cumplimiento y los textos con las condiciones operativas de obligado cumplimiento que servirán de base para la seguridad en la ejecución de los contratos con proveedores.

La OGS verificará periódicamente el cumplimiento de las políticas de relación y operación con proveedores y pondrá en marcha los procesos de auditoría que sean necesarios para verificar que se cumplen los requisitos establecidos.

### **4.1.2 Capacidad: GESTIÓN, REPORTE Y CONTROL**

#### **Servicios a prestar:**

##### **4.1.2.1 Reporte a Comités y Organismos**

La OGS definirá y ejecutará el modelo de comunicación para el reporte de información a comités y organismos, de modo que se definan los interlocutores autorizados y se establezcan los adecuados canales de comunicación. Se concretará la información a reportar, la periodicidad de los informes así como su contenido estándar y su formato.





La acción de reporte proporcionará además un mecanismo para informar a las entidades externas que así lo requieran, bien como parte de la obligada rendición de cuentas o cuando exista colaboración con otros organismos para tareas de gestión de la seguridad y control del riesgo, cuando estos trabajos se realicen de manera conjunta.

#### **4.1.2.2 Comunicación**

La OGS definirá los canales de comunicación que habiliten el necesario intercambio de información entre los distintos agentes implicados en la gestión de la seguridad (Unidades organizativas de la propia Agencia, clientes, ciudadanos, Fuerzas y Cuerpos de Seguridad del Estado,...etc.)

Una adecuada estrategia de comunicación permitirá:

- La comunicación eficaz de objetivos, estrategias, políticas y normativa de seguridad.
- El reporte desde las áreas operativas para el seguimiento y control de los niveles de madurez de seguridad.
- El intercambio de información entre áreas para la mejora de los flujos de proceso y la optimización de los recursos disponibles.
- la comunicación con los colectivos y entidades interesadas: ciudadanos, empresas, clientes, usuarios y organismos oficiales.
- El reporte periódico de incidentes de seguridad de acuerdo a la legislación y la normativa interna.
- La colaboración con los Cuerpos y Fuerzas de Seguridad del Estado y otros organismos implicados en la detección y gestión de incidentes de seguridad.

#### **4.1.2.3 Herramientas de control y seguimiento**

La OGS aportará y desarrollará para MD las herramientas necesarias para el control de la implementación de las políticas, las estrategias y los procesos de seguridad. A modo de ejemplo, y sin que sea limitativo, se desarrollarán:

- Cuadros de mando.
- Métricas e indicadores.
- Canales de reporte vertical y horizontal.
- Informes periódicos.
- Comités de seguimiento.
- ...etc.

Y cualquier otra herramienta de control que MD necesite para el análisis del riesgo y, en general, para el seguimiento de la gestión de la seguridad.

Dichas herramientas permitirán obtener información relevante sobre la gestión del riesgo, el desempeño de la operación de seguridad y la efectividad de los controles implementados. Con ellas se dará soporte a la toma de decisiones.

#### **4.1.2.4 Elaboración de planes de acción y seguimiento de despliegues**

La OGS llevará a cabo la elaboración de los planes de acción que MD determine, así como el seguimiento del desarrollo y de la ejecución de los mismos. Estos planes estarán dirigidos a la gestión de riesgos y al desarrollo de planes estratégicos, tácticos u operativos en el ámbito de la seguridad. Se revisará periódicamente la planificación y su cumplimiento, de modo que se puedan identificar aquellos riesgos que puedan afectar a los resultados esperados y se realicen las acciones correctivas necesarias para su tratamiento.

Los planes de acción contemplarán distintas iniciativas como la implementación de procesos y la aplicación de controles o medidas de seguridad.



#### **4.1.3 Capacidad: CUMPLIMIENTO NORMATIVO**

##### **Servicios a prestar:**

##### **4.1.3.1 Identificación de la regulación aplicable**

La OGS se encargará de identificar todos aquellos requisitos legales y normativos que, en el ámbito de la seguridad, apliquen a la actividad de la Agencia.

Se analizará la legislación en vigor, la normativa existente y los códigos de buenas prácticas en todos ámbitos de la seguridad aplicables a MD. Se analizará el impacto normativo sobre la actividad de la Agencia y se sistematizarán y comunicarán los requisitos operativos que deban implantarse para lograr el cumplimiento legal. Se establecerán los controles necesarios para tal cumplimiento así como sus indicadores de medida.

Deberán tenerse en cuenta los diferentes niveles de seguridad requeridos en cada caso y en cada tratamiento de la información. Como ejemplo, para el cumplimiento de la regulación de protección de datos personales se identificarán los requisitos en función de la tipología de los datos, mientras que en el cumplimiento del Esquema Nacional de Seguridad se categorizarán los sistemas de información.

La revisión y el análisis normativo se harán de manera continua y permanente, de tal manera que se valore continuamente el nivel de cumplimiento de la Agencia y se propongan, si fuera necesario, nuevos requisitos a tener en cuenta o controles de seguridad adicionales.

##### **4.1.3.2 Definición de la Política de Seguridad**

La OGS definirá y propondrá la política de seguridad de la Agencia y la de la Comunidad de Madrid. Ambas políticas se revisarán periódicamente y se generarán nuevos contenidos en caso de producirse cambios sustanciales en la estrategia o en los objetivos de la ciberseguridad.

Las políticas de seguridad deberán satisfacer los requisitos legales y normativos que sean de aplicación, y estarán alineadas con las directrices de MD y de la Comunidad de Madrid en el ámbito de la seguridad. Las políticas de seguridad recogerán los principios básicos de la seguridad a tener en cuenta y los criterios fundamentales para su aplicación.

##### **4.1.3.3 Definición de la normativa de seguridad**

La OGS definirá los contenidos, los formatos y la estructura documental necesaria para el desarrollo normativo y documental de la política de seguridad. Se elaborará un cuerpo normativo de seguridad de alto nivel y se sentarán las bases para el desarrollo del resto de procedimientos y guías técnicas de rango inferior.

Se darán directrices y se establecerán los requisitos concretos a tener en cuenta. Se definirá el conjunto documental que deberá conformar el cuerpo normativo y se establecerán los contenidos mínimos a desarrollar para garantizar que la operación cuenta con la madurez requerida.

Se realizará un seguimiento del desarrollo del cuerpo normativo, en el que se verificará que se documentan de manera apropiada los procedimientos y procesos de seguridad y que la operación está alineada con la normativa.

##### **4.1.3.4 Definición de planes de formación y concienciación**

La OGS definirá los objetivos de formación y concienciación para cada uno de los colectivos que se hayan identificado previamente.

A partir de dichos objetivos se definirán los contenidos a desarrollar y las distintas líneas de actuación a incluir en los planes de formación y concienciación.

La OGS desarrollará los contenidos documentales y audiovisuales que sean necesarios para dar forma a los diferentes planes de formación y concienciación.



Se realizará un seguimiento de que las actividades formativas y de concienciación se desarrollan adecuadamente y contribuyen a mejorar la seguridad en los procesos. Se definirán los indicadores de medición de la efectividad de los planes de formación y concienciación y se aplicarán para la valoración de resultados.

## **4.2 Ámbito: PREVENCIÓN**

### **4.2.1 Capacidad: PROCEDIMIENTOS Y PROCESOS DE PROTECCIÓN**

#### **Servicios a prestar:**

#### **4.2.1.1 Asesoramiento en seguridad**

La OGS proporcionará servicios de consultoría de seguridad legal y en el ámbito de seguridad en las TIC. Se prestará asesoramiento a las Áreas de MD y a clientes de la Comunidad de Madrid que no dispongan de los recursos o la experiencia necesarios para un desarrollo adecuado de seguridad en sus operaciones.

A modo de ejemplo, deberá proporcionarse asesoramiento en los siguientes aspectos:

- Prevención de Riesgos Laborales.
- Protección de datos personales: Adecuación a la LOPD y Reglamento Europeo sobre Protección de Datos (RGPD).
- Análisis de riesgos y evaluaciones de impacto (EIPD) según Reglamento Europeo de Protección de Datos.
- Definición de requisitos de seguridad a partir de normativa o legislación en vigor.
- Asesoramiento en Esquema Nacional de Seguridad, Ley de Protección de Infraestructuras Críticas y otra legislación aplicable.
- Definición de métricas e indicadores de seguridad.
- Buenas prácticas en gestión de la seguridad, comunicados, concienciación y formación.
- Definición de políticas de seguridad, normativa sobre firma electrónica y certificados.
- Reglamento Europeo sobre identificación electrónica y servicios de confianza.
- Normativa de seguridad para la administración electrónica.

El modo y el nivel de servicio para la prestación del asesoramiento legal lo establecerá MD a la OGS en cada caso.

#### **4.2.1.2 Tratamiento de excepciones de seguridad**

En caso de requerirse la ejecución de acciones, asignación de permisos, configuración de activos TIC u otras situaciones que contravengan la política, la normativa o los procedimientos de seguridad definidos; la OGS realizará la gestión y el tratamiento de dichas excepciones con el fin de asegurar su documentación, registro, autorización y regulación.

Se establecerán los responsables para la autorización de excepciones de seguridad, de modo que dichos responsables tengan en cuenta el riesgo derivado de las mismas. Se definirán los formatos documentales apropiados y se establecerá también una tipología para las excepciones de seguridad que permita asociar la identificación de dichos responsables.

### **4.2.2 Capacidad: PROTECCIÓN DE LA INFRAESTRUCTURA**

#### **Servicios a prestar:**

#### **4.2.2.1 Protección ambiental y áreas seguras**

La OGS identificará los riesgos de seguridad ambiental y laborales, determinando los controles a implementar en función de la clasificación de las áreas en las que el personal realice sus funciones teniendo en cuenta los procesos que se lleven a cabo y la información que se trate en dichas áreas, así como el nivel de seguridad que pueda afectar al personal implicado en el acceso a las mismas o en las operaciones.



Se asegurará que la implementación de los requisitos de seguridad se realiza de manera adecuada y que cumple con los parámetros que se hayan establecidos. Se asegurará de esta manera que las instalaciones que se albergan información o personas satisfacen los requisitos de seguridad establecidos.

La OGS identificará los riesgos de las infraestructuras críticas, los escenarios de riesgo y definición de los planes de tratamiento de riesgos de los activos de MD en relación con las infraestructuras críticas (Ley 8/2011, de 28 de abril y desarrollo reglamentario) de la Comunidad de Madrid en las que Madrid Digital opere o preste servicio.

#### **4.2.3 Capacidad: PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN**

##### **Servicios a prestar:**

##### **4.2.3.1 Requisitos de seguridad en sistemas de información**

La OGS identificará aquellos requisitos de seguridad que, derivados tanto del marco normativo legal como de la regulación interna, deban ser aplicable al desarrollo o la adquisición de sistemas de información.

Se prestará el soporte necesario para la identificación, definición e implementación de los requisitos de seguridad con el objetivo de que se realice de manera adecuada y que cumpla con los parámetros que se hayan establecidos. Este control se realizará durante las etapas de diseño y de construcción y, en cualquier caso, antes del paso a producción de los sistemas de información.

Se asegurará de esta manera que los SSII que se ponen en producción tienen asociada una correcta declaración de aplicabilidad de los requisitos de seguridad según la naturaleza y características del servicio que soportan y de la información que trata.

#### **4.2.4 Capacidad: GESTIÓN DE IDENTIDADES Y ACCESOS**

##### **Servicios a prestar:**

##### **4.2.4.1 Seguridad en la identidad digital**

La OGS definirá los requisitos de seguridad del Modelo de Identidad Digital de la Comunidad de Madrid, de modo que se asegure el cumplimiento de la normativa aplicable y se garantice la aplicación de medidas de seguridad e la identificación de las personas, la autenticación, la gestión de credenciales, la gestión de perfiles, el ciclo de vida de las claves, la firma digital y cualquier otro aspecto que en este ámbito sea relevante.

Se desarrollará cuanta normativa interna sea necesaria en relación con la identidad digital y los procesos de seguridad asociados a la misma.

##### **4.2.4.2 Seguridad en el acceso físico**

La OGS establecerá aquellos requisitos de seguridad que, derivados tanto del marco normativo legal como de la regulación organizativa interna relativas al control de acceso físico a edificios e instalaciones, y que tendrán en cuenta la clasificación de las distintas áreas. Los controles de acceso físico implantados deberán garantizar que se cumplen los requisitos para el acceso a la información y a los procesos.

Se asegurará que la implementación de los requisitos de seguridad en los sistemas de seguridad se realiza de manera adecuada y que cumple con los requisitos de seguridad y parámetros de configuración y trazabilidad que se hayan establecidos.

#### **4.2.5 Capacidad: FORMACIÓN Y CONCIENCIACIÓN**



## **Servicios a prestar:**

### **4.2.5.1 Formación y concienciación en seguridad y prevención de riesgos laborales para la Dirección**

La OGS diseñará y llevará a cabo los planes de formación y concienciación que se consideren necesarios para cubrir las necesidades específicas de la Dirección de MD o de la CM en materia de seguridad y asesoramiento legal.

Se proporcionarán los recursos necesarios para prestar a la Dirección de MD o de la CM una formación en aquellos aspectos de la seguridad y de prevención de riesgos laborales más relevantes para sus funciones, realizando al mismo tiempo actividades de concienciación que fomenten el conocimiento de la importancia y el valor estratégico de la seguridad.

Se proporcionará formación específica para la Dirección en cuestiones legales, análisis y asunción de riesgos, continuidad de negocio, protección de datos y políticas de seguridad.

La OGS desarrollará los contenidos documentales y audiovisuales que sean necesarios para dar forma a los diferentes planes de formación y concienciación.

### **4.2.5.2 Formación y concienciación en seguridad para el personal**

La OGS diseñará y ejecutará los planes de formación y concienciación que se consideren necesarios, enfocados a las necesidades específicas del personal. Se proporcionarán los recursos necesarios para prestar al personal una formación en aquellos aspectos de la seguridad más relevantes para sus funciones, realizando al mismo tiempo actividades de concienciación que fomenten el conocimiento de la importancia de la seguridad.

Se proporcionará formación específica en protección de datos, seguridad en las operaciones, ingeniería social, uso de certificados y claves, uso de medios electrónicos y correo electrónico, navegación por Internet, prevención de incidentes y prevención de riesgos laborales.

La OGS desarrollará los contenidos documentales y audiovisuales que sean necesarios para dar forma a los diferentes planes de formación y concienciación.

### **4.2.5.3 Ciudadanos y campañas de comunicación**

La OGS proporcionará al público objetivo establecido en los planes de formación y concienciación los recursos de formación de seguridad que se consideren necesarios para el cumplimiento de las líneas de actuación de Ciberseguridad de la CM y sus programas de desarrollo. Se promoverán actuaciones de fortalecimiento de las capacidades de prevención, detección y respuesta a ciberataques por parte de los usuarios de los sistemas de información. Podrán formar parte del público objetivo tanto usuarios, como ciudadanos y empresas.

Se diseñarán y ejecutarán prioritariamente aquellas campañas de comunicación que estén dirigidas a mejorar el nivel de concienciación y que logren un mayor impacto y penetración en el público objetivo.

## **4.2.6 Capacidad: SEGURIDAD DE LOS RRHH**

### **Servicios a prestar:**

#### **4.2.6.1 Seguridad en relaciones laborales**

La OGS diseñará los controles de seguridad a aplicar en los procesos de contratación de personal, tanto en las actuaciones previas a la formalización de los contratos como a lo largo de la relación laboral y a la finalización de la misma. Dichos controles asegurarán la idoneidad del personal para las tareas a desempeñar, de modo que se asegure el cumplimiento de los requisitos de seguridad que se hayan establecido previamente en este ámbito.



En el momento de la contratación y dependiendo del perfil del empleado, se definirán las condiciones específicas de contratación y se requerirá la firma de un clausulado específico que recoja los términos de seguridad en aspectos como la independencia profesional, el tratamiento de los conflictos de interés, la inhabilitación para determinados cargos, ...etc.

De igual modo, se establecerán las cláusulas aplicables a la finalización de la relación laboral relacionadas con el deber de no revelar información sensible o confidencial.

#### **4.2.6.2 Prevención, gestión de riesgos e incidentes laborales**

La OGS dará el soporte necesario para una adecuada gestión de la acción preventiva mediante la evaluación de riesgos laborales, la planificación de la actividad, y un seguimiento continuo de las actividades preventivas incluidas en la planificación. Se ejecutarán las actividades necesarias para una gestión adecuada de la acción preventiva de la Agencia, que deberán incluir planes de formación y de prevención.

La OGS deberá elaborar, mantener y conservar la documentación referida en el artículo 23 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales, así como cualquier otra relativa a las obligaciones establecidas en la normativa de prevención de riesgos, cuando así se determine por la Agencia.

La OGS realizará la gestión de incidentes laborales, que incluirán la notificación, la priorización, la resolución, el escalado y documentación. Cuando se haya producido un daño para la salud de los trabajadores o cuando aparezcan indicios de que las medidas de prevención resultan insuficientes, llevará a cabo una investigación al respecto, a fin de detectar las causas de estos hechos.

#### **4.2.6.3 Seguridad física de las personas**

La OGS diseñará e implementará aquellas medidas de seguridad encaminadas a preservar la integridad física de las personas en el desempeño de sus funciones laborales para la Agencia. Comprobará que los sistemas de seguridad instalados y las empresas de seguridad privada contratadas cumplen con las exigencias de homologación de los organismos competentes.

La OGS comprobará el cumplimiento normativo de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada y normativa organizativa interna. Se analizará los riesgos y vulnerabilidades de los equipos físicos y lógicos gestionados por el Servicio de Seguridad de la Agencia, esto es control de accesos, de intrusión y detección-extinción de fuego.

Se tendrán en cuenta para ello las clasificaciones previamente realizadas de las áreas de trabajo, la normativa en prevención de riesgos laborales y otros aspectos o normativas que se consideren aplicables.

### **4.3 Ámbito: DETECCIÓN**

#### **4.3.1 Capacidad: PROCEDIMIENTOS Y PROCESOS DE DETECCIÓN**

##### **Servicios a prestar:**

##### **4.3.1.1 Relación con agentes externos**

La OGS establecerá los canales de comunicación e identificará a los interlocutores necesarios para la colaboración con los agentes externos en el proceso de detección de amenazas e incidentes.

Para la detección de incidentes se contará principalmente con el apoyo de las Fuerzas de Seguridad y con organismos oficiales como el CCN-CERT o autoridades de control en materia de datos personales como la AEPD. Se definirán, para cada tipo de incidente o amenaza, los canales más apropiados para su gestión de manera que ésta se lleve a cabo de la forma más adecuada y ágil.





#### 4.3.1.2 Colaboración con Fuerzas y Cuerpos de Seguridad del Estado

La OGS definirá en el ámbito de la organización de seguridad los canales de comunicación que permitan habilitar el intercambio de información entre los distintos agentes implicados en seguridad: Agencia Madrid Digital, clientes, ciudadanos, Fuerzas y Cuerpos de Seguridad del Estado,...etc.)

La estrategia de comunicación permitirá definir:

- La comunicación de objetivos, estrategias, políticas y normativa para su cumplimiento.
- El reporte de las áreas de MD para el seguimiento y control de los niveles de madurez de seguridad por parte de la OGS.
- El intercambio de información entre áreas para la mejora de los flujos de los procesos y la optimización de los recursos disponibles.
- La comunicación con los distintos colectivos y entidades: ciudadanos, empresas, clientes, usuarios y Organismos oficiales.
- El reporte periódico de incidentes de seguridad de acuerdo a la legislación y la normativa interna de MD.
- La colaboración con los Cuerpos y Fuerzas de Seguridad del Estado y otros Organismos para la detección y gestión de incidentes.

#### 4.4 Ámbito: RESPUESTA Y RECUPERACIÓN

##### 4.4.1 Capacidad: RESPUESTA ANTE INCIDENTES

###### Servicios a prestar:

##### 4.4.1.1 Análisis y peritaje forense

La OGS proporcionará servicios de análisis y peritaje forense y legal, que incluirán aspectos como:

- La extracción y la gestión y custodia de la información extraída.
- La preservación de pruebas.
- La garantía del no repudio y la constitución de la cadena de custodia.
- El cumplimiento de la normativa legal aplicable en cada caso.
- El tratamiento forense de incidentes de seguridad mediante la revisión de logs, trazas y otras huellas de auditoría.
- La ejecución de los informes periciales necesarios en cada caso.
- El soporte jurídico de tipo forense que md precise en cada caso.
- La elaboración de análisis e informes periciales forenses para md y su exposición en procesos judiciales en los que la Comunidad de Madrid o la Agencia pueda intervenir como parte.

##### 4.4.2 Capacidad: ASEGURAMIENTO DE LA CONTINUIDAD

###### Servicios a prestar:

##### 4.4.2.1 Definición y mantenimiento de Planes de Continuidad

La OGS definirá un Plan de Recuperación de Desastres (**DRP**) y un Plan de Continuidad de Negocio (**BCP**) a partir del análisis de impacto sobre la actividad de la Agencia (**BIA**) que ella misma elaborará.

Para ello, Madrid Digital, a través de la OGS, identificará los servicios y activos más críticos, así como los escenarios de mayor riesgo para la Agencia atendiendo tanto a criterios de probabilidad como de impacto.

Los planes definidos deberán documentar las acciones a ejecutar y las áreas y las personas implicadas en la recuperación de la operación en caso de incidente, dentro de los parámetros establecidos en el Plan y con los controles de seguridad que se hayan acordado.





Se definirá un calendario de revisión del contenido de los planes, que deberán actualizarse periódicamente o siempre que se produzcan cambios significativos en la Agencia.

#### 4.4.2.2 Gestión de crisis

La OGS diseñará y establecerá los mecanismos de respuesta necesarios para la gestión de situaciones de crisis, de modo que el proceso de toma de decisiones en caso de un incidente que pueda afectar a la continuidad de los servicios se realice de forma adecuada.

Se definirá la composición de los comités de crisis necesarios, de modo que sus integrantes cuenten con los conocimientos, el asesoramiento y la capacidad de decisión necesarios para una gestión correcta y, si procede, la ejecución de los Planes de Recuperación de Desastres y/o Planes de Continuidad de Negocio.

La gestión de crisis deberá contribuir a la mejora continua de los procesos de prevención, detección, respuesta y recuperación, mediante la identificación y documentación de ineficiencias o aspectos a corregir.

En el caso de violación grave de la seguridad de la información, la OGS llevará a cabo las actividades vinculadas a las capacidades de gobierno que sean necesarias para su gestión, bajo la dirección y control de la Dirección de Seguridad Corporativa. Y en caso de que la violación de la seguridad alcance a datos personales, la OGS dará el soporte necesario para su adecuada gestión interna y la posterior notificación a la Agencia Española de Protección de Datos.

#### 4.4.2.3 Simulacros de los planes de continuidad

La OGS probará la eficacia de los Planes de Recuperación de Desastres (**DRP**) y de los Planes de Continuidad de Negocio (**BCP**) de MD y garantizará su actualización a lo largo del tiempo. Se llevarán a cabo pruebas periódicas mediante su revisión en ejercicios teóricos de verificación como mediante la ejecución de simulacros de incidente.

Se definirá una planificación de revisiones de la ejecución de cada plan, así como de los correspondientes simulacros, a partir de los cuales se identificarán aspectos de mejora y lecciones a aprender, que se utilizarán para hacer evolucionar los planes.

Se coordinará la ejecución de simulacros con los principales interesados y, en caso de requerirse, con aquellos organismos públicos y proveedores cuya participación se necesite.

#### 4.4.2.4 Aprendizaje de los simulacros de los planes de continuidad

A partir de la ejecución de simulacros y de la gestión de las eventuales crisis, la OGS realizará análisis detallados de los pasos que se hayan llevado a cabo, de los resultados obtenidos y de la disponibilidad de recursos en cada momento así como de otros factores.

A partir de estos análisis, la OGS identificará los aspectos de mejora en los procedimientos y en procesos de MD, las causas raíz de los incidentes, las vulnerabilidades y las amenazas no conocidas y las carencias de seguridad en prevención o detección que hayan podido estar involucradas.

La OGS, a través del análisis efectuado, proporcionará información relevante para la mejora de los procesos de la ciberseguridad de MD, de modo que el gobierno, la prevención, la detección y la respuesta y recuperación sean más efectivos.

### 4.5 EQUIPO DE TRABAJO

Para desempeñar los servicios objeto del pliego, el adjudicatario contará con una capacidad productiva configurada en primer lugar el equipo de trabajo **Base** y los respectivos equipos de **Proyecto** que garanticen el nivel de especialización requerido para el servicio continuo o despliegue de capacidades, y en segundo



lugar por la capacidad productiva back-office que sea necesaria aportar por parte del adjudicatario, más allá de los integrantes de los equipos antes mencionados, para alcanzar la calidad de la prestación del servicio que se establezca por la Agencia. Esta capacidad productiva back-office deberá garantizarse desde el inicio del servicio y no supondrá en ningún momento sobre coste para la Agencia.

Los equipos de trabajo garantizarán la permanencia y transferencia del conocimiento a lo largo de la duración del contrato, tanto del conocimiento transferido inicialmente por la Agencia, como del adquirido por los equipos durante la prestación de los servicios.

El servicio de la OGS se compone de:

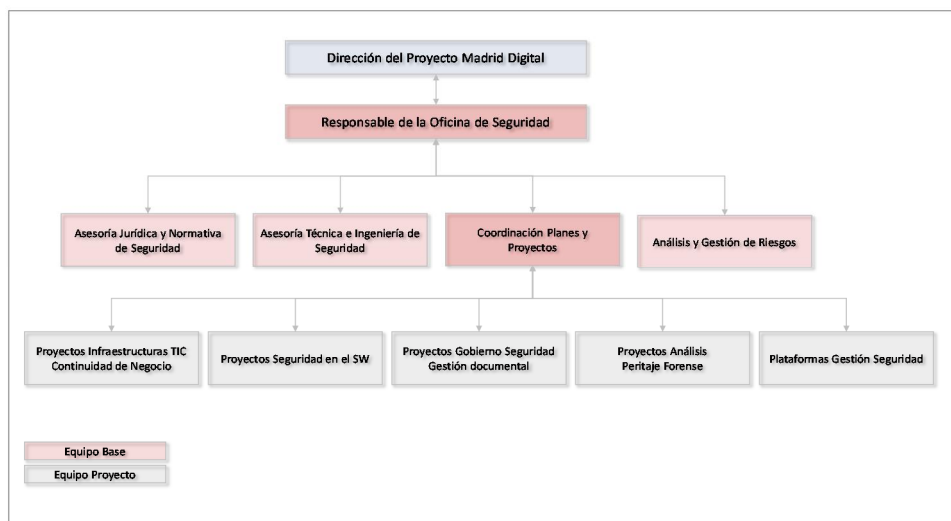
- **Gestión del Servicio Continuo** del equipo de trabajo denominado **Equipo Base**. El adjudicatario constituirá el Equipo Base con las capacidades y perfiles necesarios definidos. Este servicio estará constituido por:
  - Prestación del servicio continuo con las líneas de actuación definidas en el apartado 4.5.1.
  - Prestación del servicio continuo de coordinación para la implantación y el seguimiento de todos los planes de acción, programas de desarrollo de la seguridad y servicios continuos o de duración limitada en el tiempo.
- **Gestión de Proyectos o Servicios no planificados** del equipo de trabajo denominado **Equipo Proyecto**, para atender a las líneas de actuación o proyectos definidos, así como para dar el apoyo y soporte cuando sea necesario para atender a necesidades no planificadas planteadas por la Dirección del Proyecto. Este servicio, a demanda de MD, estará constituido por:
  - Prestación del servicio proyecto con las líneas de actuación definidas en el apartado 4.5.2.
  - Definición, desarrollo e Implantación de proyectos de servicios, planes y programas.

El número de horas estimado *a priori* por categorías para los servicios no planificados (cuota variable), y el importe estimado por anualidades es el siguiente:

<b>Gestión de Proyectos (Cuota VARIABLE) - Equipo PROYECTO</b>				
<b>DEDICACIONES por perfiles profesionales</b>				
<b>Perfiles Profesionales</b>	<b>HORAS AÑO 2019 (3 meses)</b>	<b>HORAS AÑO 2020 (12 meses)</b>	<b>HORAS AÑO 2021 (9 meses)</b>	<b>HORAS TOTALES (24 meses)</b>
Auditor Senior	405	1.621	1.215	3.241
Consultor Senior	480	1.920	1.440	3.840
Ingeniero de Seguridad	480	1.920	1.440	3.840
Analista	480	1.920	1.440	3.840
<b>HORAS TOTALES</b>	<b>1.845</b>	<b>7.381</b>	<b>5.535</b>	<b>14.761</b>
<b>IMPORTES POR ANUALIDAD. TOTAL GENERAL</b>	<b>71.235,00 €</b>	<b>284.995,00 €</b>	<b>213.705,00 €</b>	<b>569.935,00 €</b>



A continuación se resume la organización necesaria para constituir y desarrollar la actividad de la OGS:



Y esta estructura deberá prestar el servicio continuo especificado en el apartado 4.5.1 y en la cláusula cuarta referida al marco de capacidades, funciones y servicios a prestar por la OGS, relativo a:

**Capacidad: GOBIERNO Y GESTIÓN DEL RIESGO**

Gestión de activos  
Catálogo de amenazas  
Análisis de riesgos  
Análisis de auditorías y cumplimiento

**Capacidad: GESTIÓN, REPORTE Y CONTROL**

Herramientas de control y seguimiento  
Elaboración de planes de acción y seguimiento de despliegues

**Capacidad: CUMPLIMIENTO NORMATIVO**

Identificación de la regulación aplicable  
Definición de la Política de Seguridad  
Definición de la normativa de seguridad  
Definición de planes de formación y concienciación

**Capacidad: PROCEDIMIENTOS Y PROCESOS DE PROTECCIÓN**

Asesoramiento en seguridad

**Capacidad: PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN**

Requisitos de seguridad en sistemas de información

**Capacidad: GESTIÓN DE IDENTIDADES Y ACCESOS**

Seguridad en la identidad digital

**Capacidad: SEGURIDAD DE LOS RRHH**

Seguridad en relaciones laborales  
Prevención, gestión de riesgos e incidentes laborales  
Seguridad física de las personas

**Capacidad: PROCEDIMIENTOS Y PROCESOS DE DETECCIÓN**

Relación con agentes externos  
Colaboración con Fuerzas y Cuerpos de Seguridad del Estado

Así como el servicio proyecto especificado en el apartado 4.5.2 y en la cláusula cuarta referida al marco de capacidades, funciones y servicios a prestar por la OGS, relativo a:

**Capacidad: GOBIERNO Y GESTIÓN DEL RIESGO**

Seguridad en la relación con proveedores

**Capacidad: GESTIÓN, REPORTE Y CONTROL**

Reporte a Comités y Organismos

Comunicación

**Capacidad: PROCEDIMIENTOS Y PROCESOS DE PROTECCIÓN**

Tratamiento de excepciones de seguridad

**Capacidad: PROTECCIÓN DE LA INFRAESTRUCTURA**

Protección ambiental y áreas seguras

**Capacidad: GESTIÓN DE IDENTIDADES Y ACCESOS**

Seguridad en el acceso físico

**Capacidad: FORMACIÓN Y CONCIENCIACIÓN**

Formación y concienciación en seguridad y riesgos laborales para la Dirección

Formación y concienciación en seguridad para el personal

Ciudadanos y campañas de comunicación

**Capacidad: RESPUESTA ANTE INCIDENTES**

Análisis y peritaje forense

**Capacidad: ASEGURAMIENTO DE LA CONTINUIDAD**

Definición y mantenimiento de Planes de Continuidad

Gestión de crisis

Simulacros de los planes de continuidad

Aprendizaje de los simulacros de los planes de continuidad

Por todo ello, el adjudicatario pondrá a disposición de MD **dos tipos de equipos de personas: Base y Proyecto**, ambos con dedicación exclusiva para MD y con ubicación en la sede de la Agencia de la C/ Embajadores, 181. **El equipo Base, constituido al menos por 5 personas - tendrá dedicación permanente a MD.** Su dedicación será exclusiva durante todo el periodo de vigencia del contrato.

**El equipo – o los equipos – de Proyecto se constituirán ocasionalmente previa aprobación de la Dirección del Proyecto**, lo que permitirá la demanda del Jefe de proyecto, una vez constituida la OGS, para la puesta en marcha planificada de proyectos o servicios específicos del Plan de Ciberseguridad de MD. Mientras estén al servicio de la OGS su dedicación será en exclusiva.

Los equipos de Proyecto podrán constituirse en número variable de componentes, a demanda del Jefe de Proyecto, **sobre la base de cualquier combinación de perfiles profesionales contemplados en el pliego.**

**La constitución de equipos de Proyecto se avisará al adjudicatario con 7 días naturales de antelación quedando fuera de este criterio las demandas de efectivos al adjudicatario motivadas por la ocurrencia de incidentes graves, servicios especiales o eventos críticos, que serán identificados formalmente como tales por el Jefe de Proyecto. Estas demandas deberán ser atendidas inmediatamente por el adjudicatario.**

El adjudicatario se obligará a poner a disposición de MD estos recursos dentro del plazo señalado. El no cumplimiento de esta obligación, tanto en número de personas como en la cualificación profesional de las mismas, dará lugar a la penalización correspondiente. (Ver **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**).

Los equipos de Proyecto se ubicarán, con carácter general, en la sede central de MD (C/ Embajadores, 181) o en cualquiera de sus dependencias, si bien en cada momento esta ubicación física dependerá de la disponibilidad de espacio y mobiliario en MD. El Jefe de Proyecto establecerá el criterio para la ubicación de las personas en función del proyecto o servicio a cubrir por estos equipos. Este criterio se adaptará en cada momento a las disponibilidades materiales en MD.



El adjudicatario podrá solicitar que sus equipos de trabajo se ubiquen en sus propias dependencias cuando estime que la duración de la dedicación de cada persona al servicio o proyecto no vaya a superar, según su criterio, las **80 h/h**. Esta solicitud deberá ser aceptada, tanto en valoración de esfuerzo - medida en h/h y número de personas - como en el modo de prestación del servicio por el Director del Proyecto. Aún en el caso de aceptación de la valoración del esfuerzo, el Director de Proyecto podrá exigir al adjudicatario la prestación presencial del servicio en las dependencias de MD.

La cuantificación del esfuerzo, medido en h/h por persona, y del número de efectivos a cada servicio, proyecto o programa de trabajo de la OGS (tanto para el equipo Base como para los equipos de Proyecto que se constituyan) corresponderá al Jefe de Proyecto de MD, que será quien valore y cuantifique estos extremos de modo justificado y documentado, correspondiendo la designación de personas a tareas y la organización de las mismas al Coordinador de Planes y Proyectos. Esta valoración será revisada por el *Coordinador de Planes y Proyectos de la OGS* quien propondrá las modificaciones que considere oportunas. En caso de discrepancia, prevalecerá el criterio razonado y documentado del Jefe de Proyecto de MD, salvo que la desviación sea igual o superior a dos terceras partes de lo estimado por el Jefe de Proyecto, caso en el que se elevará al Comité de Seguimiento del Contrato el cual decidirá el criterio en base a los informes razonados del Jefe de Proyecto y del Coordinador de Planes y Proyectos.

El Coordinador de Planes y Proyectos cuantificará el grado de avance de cada proyecto o servicio y la asignación de personas a los mismos y propondrá al Jefe de Proyecto los cambios que considere en base a los efectivos disponibles y a los plazos comprometidos por MD en cada caso. Estos cambios, antes de llevarse a cabo, deberán ser aceptados por el Director del Proyecto.

El adjudicatario asumirá que todos los proyectos y servicios a desarrollar por la OGS deberán ser cubiertos por el equipo humano descrito en este pliego. Cualquier otro perfil profesional o recurso complementario o de soporte que la OGS necesite correrá por cuenta del adjudicatario y no podrá suponer en ningún caso un extra-coste para MD. Quedarán fuera de esta consideración aquellos servicios que por su naturaleza excepcional (por la cualificación profesional necesaria o por otras circunstancias) estén fuera del alcance de este pliego. La condición excepcional de un servicio deberá ser ratificada en cualquier caso por MD. Con independencia de su carácter excepcional o no, ningún servicio que se demande al adjudicatario relacionado con el objeto, la naturaleza y los fines de la OGS podrá valorarse a precios unitarios hora/hombre superiores a los establecidos en la adjudicación del contrato. Este criterio será aplicable a cualquier perfil que se necesite para la prestación del servicio demandado.

Los cometidos y las actividades a desarrollar por cada equipo se ajustarán a los perfiles y al conjunto de capacidades, funciones y servicios recogidos en el alcance este pliego. La definición de planes de trabajo, el contenido de los encargos, el nivel de desarrollo de las capacidades de gestión de la seguridad para MD, el modo de prestación y el nivel de calidad de los servicios será marcada por la Dirección del Proyecto en el marco del Comité de Seguimiento del Contrato.

La asignación de personas a tareas responderá a las necesidades de organización del servicio que determine el Jefe de Proyecto. Esta distribución podrá modificarse en cualquier momento durante la ejecución del contrato. La asignación de personas a los diferentes planes, servicios y proyectos será comunicada por el Coordinador de Planes y Proyectos al Jefe del Proyecto de MD. Esta asignación de personas a tareas hecha por el Coordinador de Planes y Proyectos será hecha a riesgo y ventura del adjudicatario para el cumplimiento de objetivos, plazos y resultados. De modo que cualquier incremento de recursos por circunstancias sobrevenidas para la prestación del servicio, no podrá suponer un sobre coste para el contrato.

#### 4.5.1 Equipo Base: Líneas de actuación y actividades a desarrollar.

**Orientación: Desarrollo de las capacidades, funciones y servicios permanentes a ofrecer por la OGS.**

Las líneas de actividad de servicio continuo de la OGS son las siguientes:

LINEA DE ACTIVIDAD	MISION	ACTIVIDADES
--------------------	--------	-------------





<b>Responsable de la Oficina de Seguridad</b>	Coordinación general de la OGS y de la calidad, eficacia y buen servicio de la misma.	<ul style="list-style-type: none"> <li>• Ser el interlocutor principal con la Dirección del Contrato de MD.</li> <li>• Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de los riesgos propios del contrato.</li> <li>• Garantizar que el personal asignado para la ejecución de los servicios está disponible, y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.</li> <li>• Ejercer el mando y la responsabilidad sobre el equipo de la OGS.</li> <li>• Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los acuerdos de nivel de servicio (ANS) de cada periodo.</li> <li>• Proponer las alternativas de viabilidad de las solicitudes de mejora del servicio efectuadas por el adjudicatario o por MD.</li> <li>• Revisar el estado y evolución de los planes de mejora acordados y cumplimiento de los compromisos aprobados.</li> <li>• Cualquier otro asunto que el propio de la ejecución del contrato.</li> </ul>
<b>Coordinación Planes y Proyectos</b>	Coordinación de la implantación y el seguimiento de todos los planes de acción, programas de desarrollo de la seguridad y servicios continuos o de duración limitada en el tiempo que sean encomendados a la OGS, en cumplimiento de planes de acción estratégicos o servicios permanentes de seguridad definidos en MD o impulsados por la CM.	<ul style="list-style-type: none"> <li>• Coordinar los proyectos de la OGS y ser el responsable, en último término, de la buena marcha de los trabajos.</li> <li>• Ser el interlocutor principal con los Jefes de Proyecto de MD.</li> <li>• Realizar la planificación general de los trabajos de la OGS.</li> <li>• Asegurar la ejecución de las operaciones diarias de la OGS según los ANS establecidos.</li> <li>• Gestionar problemas e incidencias en las operaciones de la OGS que puedan comprometer la buena marcha de la misma y garantizar que se gestionen adecuadamente.</li> <li>• Asegurar la formación continua de los integrantes de la OGS.</li> <li>• Asegurar el conocimiento y el cumplimiento de la normativa y procedimientos de seguridad de MD por parte de los integrantes de la OGS.</li> <li>• Garantizar la integración de todos los trabajos de la OGS con las herramientas de MD y el correcto desempeño profesional del equipo humano puesto por el adjudicatario al servicio del contrato.</li> <li>• Responsabilizarse sobre el adecuado funcionamiento y la disponibilidad de las herramientas de trabajo del adjudicatario puestas al servicio de la OGS.</li> <li>• Responsabilizarse del buen uso de los medios productivos puestos por MD para el funcionamiento de la OGS.</li> <li>• Gestionar junto a cada despliegue la valoración de su avance a través de los correspondientes indicadores y cuadros de mando. Dispondrá para ello de las herramientas necesarias, que aportará el adjudicatario (Apartado 4.7 TECNOLOGÍAS Y HERRAMIENTAS).</li> </ul>
<b>Asesoría Jurídica y Normativa de Seguridad</b>	Asesoramiento, soporte especialista y ejecución de los trabajos en materia legal a MD y a la Comunidad de Madrid sobre las leyes, reglamentos y códigos de buenas prácticas en materia de seguridad de la información y prevención de riesgos laborales, incluyendo toda su normativa de desarrollo y normativa organizativa derivada.	<ul style="list-style-type: none"> <li>• Estudiar y resolver los problemas legales relacionados con la seguridad de la información y protección de datos.</li> <li>• Estudiar y resolver los problemas legales relacionados con la prevención de riesgos laborales e infraestructuras de la Agencia.</li> <li>• Emitir informes jurídicos sobre las distintas materias relacionadas en el ámbito de la seguridad (de la información y de prevención de riesgos laborales).</li> <li>• Redactar cláusulas, contratos y acuerdos relacionados con la seguridad.</li> <li>• Asesorar en materia de seguridad, dando respuesta jurídica y documental de todo tipo de gestión de derechos, declaraciones u obligaciones en materia de seguridad.</li> <li>• Participar en la realización de análisis de riesgos, en la evaluación de impacto de protección de datos.</li> <li>• Elaboración de las normas, procedimientos, guías, instrucciones y demás documentos de seguridad a elaborar por la OGS.</li> <li>• Asegurar que las normas, procedimientos, guías, instrucciones y demás documentos de seguridad a elaborar por la OGS se adecúan a la distinta normativa legal aplicable.</li> <li>• Participar en los grupos de trabajo y comités que se requiera desde la Dirección del Contrato.</li> <li>• Actualizar y mantener los repositorios documentales y sistemas de gestión asociados a la actividad.</li> </ul>



<b>Análisis y Gestión de Riesgos</b>	Asesoramiento, soporte especialista y ejecución de trabajos a realizar en el ámbito de la gestión de riesgos de los SS.II. y de los elementos comunes e infraestructura TIC de Madrid Digital en el marco de los servicios de la Oficina.	<ul style="list-style-type: none"> <li>• Mantenimiento y actualización de toda la documentación referente a la metodología, al ciclo de gestión de riesgos de MD y a todos sus componentes.</li> <li>• Mantenimiento, levantamiento y documentación de los activos de Madrid Digital.</li> <li>• Mantenimiento, evaluación y documentación del catálogo de amenazas.</li> <li>• Mantenimiento, evaluación y asignación de los valores de impacto.</li> <li>• Mantenimiento y documentación de los catálogos de las medidas de seguridad.</li> <li>• Revisión y evaluación del grado de madurez de las medidas de seguridad aplicables.</li> <li>• Determinación de los escenarios de riesgo de los SS.II. y de los elementos comunes y de infraestructuras de Madrid Digital.</li> <li>• Elaboración de los Planes de Tratamiento de Riesgos.</li> <li>• Coordinación con otros intervinientes de la ejecución de los Planes de Tratamiento de Riesgos.</li> <li>• Asesoramiento, determinación de los escenarios de riesgo y definición de los Planes de Tratamiento de Riesgos de los activos de MD en relación con las infraestructuras críticas (Ley 8/2011, de 28 de abril y desarrollo reglamentario) de la Comunidad de Madrid.</li> </ul>
<b>Asesoría Técnica Ingeniería de Seguridad</b>	Asesoramiento, soporte especialista y ejecución de los diferentes trabajos a realizar en el ámbito técnico e ingeniería de la seguridad de los servicios de la Oficina.	<ul style="list-style-type: none"> <li>• Definición, prescripción, validación y supervisión de los proyectos de seguridad con base tecnológica, generando la normativa técnica de los proyectos que se determinen en materia de seguridad.</li> <li>• Revisar o validar la certificación de seguridad de aplicaciones y productos o servicios.</li> <li>• Generación de documentación gráfica o audiovisual: planos, esquemas, presentaciones, vídeos...etc. en cualquier formato electrónico de tipo gráfico, de audio o de video homologado por Madrid Digital.</li> <li>• Generación y edición de contenidos para su publicación en páginas WEB.</li> <li>• Gestión de la publicación de contenidos en páginas WEB.</li> <li>• Gestión de los entornos de trabajo colaborativo de la OGS.</li> <li>• Llevanza del archivo electrónico y del archivo en papel de toda la documentación de la OGS, según los criterios que establezca el Jefe de Proyecto.</li> <li>• Programación, edición y gestión de puesta en producción de formularios electrónicos WEB, en cualquier formato homologado o compatible con los empleados en MD.</li> <li>• Programación interna avanzada de documentación ofimática del entorno MS-Office (Word, Excel, Power-point,...etc.), en cualquier formato y versión homologada o compatible con los empleados en MD.</li> <li>• Mantenimiento operativo y soporte funcional de la Plataforma Técnica de Gestión Documental de la Oficina.</li> <li>• Mantenimiento operativo y soporte funcional de la plataforma de generación y edición de contenidos WEB: Portal WEB de Gobierno de la Seguridad.</li> </ul>

El equipo base se conformará, con dedicación exclusiva, de al menos cinco (5) recursos, que deberán cumplir con carácter de mínimos el perfil profesional requerido para cada línea de actividad de la OGS:

LINEA DE ACTIVIDAD	EXPERIENCIA	TITULACION	FORMACION COMPLEMENTARIA	PERFIL
<b>Responsable de la Oficina de Seguridad</b>	Al menos siete (7) años de experiencia como responsable de equipos de trabajo de Seguridad de la Información y/o Ciberseguridad para	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática,	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager) o	<b>Consultor Senior</b>





	organizaciones, públicas o privadas, de tamaño igual o superior a Madrid Digital y cuya actividad sea equivalente en naturaleza, volumen y alcance a la de la Agencia.	Telecomunicaciones Matemáticas.	o CISA (Certified Information Security Auditor) de la organización ISACA.	
<b>Coordinación y Planes y Proyectos</b>	Al menos siete (7) años de experiencia como responsable de equipos de trabajo de Seguridad de la Información y/o Ciberseguridad para organizaciones, públicas o privadas, de tamaño igual o superior a Madrid Digital y cuya actividad sea equivalente en naturaleza, volumen y alcance a la de la Agencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager) o CISA (Certified Information Security Auditor) de la organización ISACA.	<b>Jefe de Proyecto</b>
<b>Asesoría Jurídica y Normativa de Seguridad</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado en Derecho o equivalente.	Deberá disponerse de formación de postgrado o Máster en Derecho de las TIC (tanto en derecho nacional como de la UE), en protección de datos y Certificación en Gestión de Seguridad de la Información (Certified Information Security Manager, CISM).  Deberá disponerse de formación de postgrado o Máster en Prevención de Riesgos Laborales.	<b>Consultor Senior</b>
<b>Análisis y Gestión de Riesgos</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager) o CISA (Certified Information Security Auditor) de la organización ISACA.	<b>Consultor Senior</b>
<b>Asesoría Técnica e Ingeniería de Seguridad</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM (Certified Information Security Manager) o CISA (Certified Information Security Auditor) de la organización ISACA.	<b>Ingeniero (Seguridad, Calidad, Sistemas, Comunicaciones, BBDD)</b>



#### 4.5.2 Equipo Proyecto: Líneas de actuación y actividades a desarrollar.

**Orientación: Implantación de proyectos y desarrollo de servicios, planes y programas, a demanda de MD.**

Las líneas de actividad de servicio proyectos o no planificados de la OGS son las siguientes:

LINEA DE ACTIVIDAD	MISION	ACTIVIDADES
<b>Proyectos Infraestructuras TIC y BCP</b>	Asesoramiento, soporte especialista y ejecución de los diferentes trabajos a realizar en el ámbito técnico de la seguridad de las infraestructuras TIC y Continuidad de Negocio dentro de los servicios de la Oficina.	<ul style="list-style-type: none"> <li>• Soporte especializado y asesoramiento técnico para definición de la seguridad de arquitectura de sistemas.</li> <li>• Asesoramiento técnico y soporte en bastionado y configuración de infraestructuras de redes y comunicaciones y de sistemas de información,</li> <li>• Soporte y gestión para la definición del Plan de Recuperación de Desastres (DRP) y del Plan de Continuidad de Negocio (BCP) de MD a partir del análisis de impacto sobre la actividad de negocio (BIA) de la Agencia.</li> <li>• Definición y gestión de los planes de prueba de la eficacia de ambos planes (DRP y DCP) a partir de la ejecución de los correspondientes simulacros.</li> <li>• Especial relevancia en las siguientes tecnologías: Servidores web y de aplicaciones (Apache, IIS, Oracle web caché, Jboss, Tomcat, Weblogic), Directorio Activo, LDAP, Sistema de Gestión de Contenidos (Joomla, Fatwire, Drupal) y Sistemas Operativos, Sistemas Gestores de Base de Datos y lenguajes de programación, en especial, Unix, Windows, Oracle forms, Delphi, java, php, Oracle, SQL Server, Informix, MySQL.</li> </ul>
<b>Proyectos Seguridad en el SW</b>	Asesoramiento, soporte especialista y ejecución de los diferentes trabajos a realizar en el ámbito técnico de la seguridad del software dentro de los servicios de la Oficina.	<ul style="list-style-type: none"> <li>• Soporte especializado y asesoramiento técnico en la seguridad del ciclo de vida del desarrollo software de sistemas de información y/o en operación.</li> <li>• Asesoramiento técnico y soporte la calidad de los requisitos, especificaciones y diseño del sistemas de seguridad de infraestructuras de redes y comunicaciones y de sistemas de información,</li> <li>• Soporte especializado y asesoramiento técnico en realización de tests de penetración y en la ejecución de hacking ético.</li> <li>• Especial relevancia en las siguientes tecnologías: Servidores web y de aplicaciones (Apache, IIS, Oracle web caché, Jboss, Tomcat, Weblogic), Directorio Activo, LDAP, Sistema de Gestión de Contenidos (Joomla, Fatwire, Drupal) y Sistemas Operativos, Sistemas Gestores de Base de Datos y lenguajes de programación, en especial, Unix, Windows, Oracle forms, Delphi, java, php, Oracle, SQL Server, Informix, MySQL.</li> </ul>
<b>Proyectos Gobierno Seguridad Documentalista</b>	Asesoramiento, soporte especialista y ejecución de los diferentes trabajos a realizar en el ámbito técnico de la seguridad de las capacidades de gestión, gobierno y control de la seguridad dentro de los servicios de la Oficina.	<ul style="list-style-type: none"> <li>• Definición, mantenimiento y actualización de herramientas de control y seguimiento.</li> <li>• Definición, mantenimiento y actualización de herramientas de gestión de la capacidad y planificación.</li> <li>• Gestión de la comunicación organizativa en materia de seguridad.</li> <li>• Definición, mantenimiento y actualización de herramientas de documentación y reporte a comités y organismos.</li> <li>• Coordinación de despliegue de despliegue de procesos de seguridad y marcos de control (cuadros de mando, informes periódicos, etc.).</li> <li>• Seguimiento de despliegue de planes de acción enfocados a la gestión de riesgos en el ámbito de la seguridad.</li> <li>• Generación documental de las normas, procedimientos, guías, instrucciones y demás documentos de seguridad a</li> </ul>



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: **1019629385769945216829**

		desarrollar por la Oficina, según directrices del Jefe de Proyecto.
		<ul style="list-style-type: none"> <li>• Gestión documental derivada de la aplicación de la normativa de seguridad en la actividad diaria de MD: Revisión de peticiones y solicitudes, generación de escritos de contestación, archivo documental,...etc.</li> <li>• Generación de documentación para su utilización en planes formativos o de concienciación sobre seguridad.</li> </ul>
<b>Proyectos</b>	Obtención, análisis e interpretación de las posibles evidencias digitales en los sistemas de información o sobre cualquier soporte digital objeto de un incidente de seguridad.	<ul style="list-style-type: none"> <li>• Obtención, análisis e interpretación de las posibles evidencias digitales en los sistemas de información objeto de un incidente de seguridad, que podrán incluir, entre otros, ordenadores, PDA's, teléfonos móviles así como otros dispositivos susceptibles de ser analizados.</li> </ul>
<b>Análisis y Peritaje Forense</b>		
<b>Plataformas Gestión Seguridad</b>	Administración, mantenimiento, evolución y operación diaria de las plataformas SW que MD decida implantar para el soporte al gobierno de la seguridad.	<ul style="list-style-type: none"> <li>• Administración de los sistemas</li> <li>• Análisis y definición funcional de los evolutivos SW necesarios para la adecuación de las plataformas SW</li> <li>• Documentación de los estudios de análisis funcional y de requisitos para la implementación y gestión de evolutivos SW en función de la normativa interna de MD</li> <li>• Seguimiento de la implantación de evolutivos y revisión de protocolos de pruebas</li> <li>• Recepción, tramitación y seguimiento de solicitudes de altas y bajas de usuarios y de las modificaciones de sus perfiles</li> <li>• Prestación de soporte funcional a usuarios y Áreas Técnicas y de Servicios de MD</li> <li>• Prestación de soporte de 3er nivel (nivel funcional experto) al Centro de Atención a Usuarios (CAU) de MD</li> <li>• Recepción, tratamiento y resolución de incidencias y consultas y tramitación con el CAU de MD</li> <li>• Mantenimiento de catálogos internos</li> <li>• Documentación, tramitación y seguimiento, con las Áreas de Desarrollo, Técnicas y de Servicios de MD, de los evolutivos SW necesarios, definidos por el Jefe del Proyecto</li> <li>• Generación de documentación del sistema: Manuales de usuario, presentaciones, guías de uso, contenidos para cursos de formación,...etc.</li> <li>• Especial relevancia en las siguientes plataformas SW actualmente en funcionamiento son: SRPD - Sistema del Responsable de Protección de Datos (en proceso de adaptación al nuevo RGPD de la UE), SGUR - Sistema para el Almacenamiento y explotación de las Trazas de Seguridad (en proceso de adaptación al nuevo RGPD de la UE), SENS - Soporte a las Especificaciones de normalización de la seguridad (en proceso de adaptación al nuevo RGPD de la UE, a la nueva LOPD y a la normativa específica de aplicación al ámbito de los sistemas de información judiciales).</li> </ul>

Los perfiles que compongan los equipos de cada proyecto, deberán cumplir con carácter de mínimos los requisitos requeridos definidos a continuación:

LINEA DE ACTIVIDAD	EXPERIENCIA	TITULACION	FORMACION COMPLEMENTARIA	PERFIL
<b>Proyectos Infraestructuras TIC y BCP</b>	Al menos cinco (5) años en las actividades ligadas a la línea de	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM ( <i>Certified Information Security Manager</i> ) o CISA ( <i>Certified Information</i>	<b>Ingeniero (Seguridad, Calidad, Sistemas, Comunicaci</b>



actuación de  
referencia.

Security Auditor) de la ones,  
organización ISACA. BBDD)

<b>Proyectos Seguridad en el SW</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM ( <i>Certified Information Security Manager</i> ) o CISA ( <i>Certified Information Security Auditor</i> ) de la organización ISACA.	<b>Ingeniero (Seguridad, Calidad, Sistemas, Comunicaciones, BBDD)</b>
<b>Proyectos Gobierno - Seguridad Documentalista</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM ( <i>Certified Information Security Manager</i> ) o CISA ( <i>Certified Information Security Auditor</i> ) de la organización ISACA.	<b>Consultor Senior</b>
<b>Proyectos Análisis y Peritaje Forense</b>	Al menos cinco (5) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM ( <i>Certified Information Security Manager</i> ) o CISA ( <i>Certified Information Security Auditor</i> ) de la organización ISACA.	<b>Auditor Senior</b>
<b>Plataformas Gestión Seguridad</b>	Al menos tres (3) años en las actividades ligadas a la línea de actuación de referencia.	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.	Deberá disponer de alguna de las siguientes acreditaciones de seguridad: CISM ( <i>Certified Information Security Manager</i> ) o CISA ( <i>Certified Information Security Auditor</i> ) de la organización ISACA.	<b>Analista / Técnico de Sistemas, de Comunicaciones, de BBDD</b>

A los efectos del párrafo anterior, el licitador que haya presentado la mejor oferta, con carácter previo a la adjudicación del contrato, deberá aportar el *currículum vitae* de las personas del Equipo Base asignadas a la ejecución del contrato, que deberá estar debidamente cumplimentado y firmado por la persona que ostente la representación a estos efectos de la empresa, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).

#### 4.6 HORARIO Y UBICACIÓN

El horario de prestación del servicio será con carácter general de 5 d. x 8 h., en la franja horaria de 8:00 a 18:00 horas en días laborables, en modo presencial en las dependencias de Madrid Digital.

El personal de la OGS tendrá disponibilidad para desplazarse a los distintos centros dependientes de la Comunidad de Madrid que pertenezcan al ámbito de competencia de Madrid Digital.

El contratista deberá en todo momento poder garantizar los recursos humanos que satisfagan la demanda de requerimientos que se tenga durante la vigencia del contrato. Los medios de trabajo necesarios para el personal adscrito a la prestación del servicio, tales como, ordenador portátil personal, teléfonos móviles, *tablets*, licencias de software ofimático, etc., correrán a cargo de la empresa adjudicataria, a excepción del pc fijo y del puesto físico de trabajo en las dependencias de Madrid Digital, que será provisto por la Agencia.

En los casos en los que sea necesario ejecutar tareas derivadas de la confirmación de la existencia de un incidente grave de seguridad que, a criterio del Jefe de Proyecto o de la Dirección de MD, requiriera la participación de la OGS, y se precisara la realización de trabajos por parte del personal de la Oficina, o por el personal del adjudicatario que no sea de la OGS, fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, Madrid Digital no aceptará sobre-coste adicional por estas circunstancias, que deberá ser absorbido siempre por el adjudicatario.



En los casos en los que sea necesario ejecutar tareas derivadas de la confirmación de la existencia de un incidente grave de seguridad o de cualquier otro que, por su naturaleza y a criterio del Jefe de Proyecto o de la Dirección de MD, requiriera la participación inmediata o extraordinaria del personal de la OGS o el personal de back-office del adjudicatario, fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, Madrid Digital no aceptará sobre-coste adicional por estas circunstancias, que deberá ser asumido por el adjudicatario.

En las circunstancias descritas en el apartado anterior, el adjudicatario dará respuesta a MD con todos los efectivos que estén a su alcance y realizará los esfuerzos necesarios para atender las demandas de MD en todos los casos, asumiendo los costes derivados de su actuación.

#### 4.7 TECNOLOGÍAS Y HERRAMIENTAS

El adjudicatario deberá asumir a su costa la provisión, el diseño, la operación y mantenimiento de todas las herramientas SW de la OGS, tanto las de gestión como las de tipo técnico o de análisis forense, con excepción de las *Plataformas SW de Soporte al Gobierno de la Seguridad* que MD defina, que serán de su propiedad.

Preferentemente se optará por soluciones tipo *opensource*, y en todo caso estarán incluidas dentro del coste de los servicios que asuma el adjudicatario, sin que en ningún caso puedan repercutirse a MD. El adjudicatario aportará a su costa las licencias SW necesarias para el funcionamiento de las herramientas de la OGS. A la finalización del contrato todas estas herramientas SW pasaran a ser propiedad de Madrid Digital. El licitador definirá en su propuesta técnica de licitación el hardware necesario para cada herramienta, que será provisionado por Madrid Digital a la formalización del contrato.

Madrid Digital podrá exigir al adjudicatario, a la finalización del contrato la migración de todos los contenidos documentales desarrollados por la OGS <sup>(1)</sup> a plataformas propias. Podrá exigir también la integración de las herramientas SW que aporte el adjudicatario con plataformas o desarrollos propios de MD. El coste asociado al traspaso de información o de las integraciones que tuvieran que realizarse será siempre por cuenta del adjudicatario.

El adjudicatario deberá aportar, como mínimo, las siguientes herramientas:

- Una plataforma de gestión documental.
- Una herramienta para la notificación, registro y gestión de peticiones de servicio a la OGS.
- Una herramienta para el análisis y gestión del riesgo.
- Una plataforma de generación y edición de documentación gráfica.
- Una plataforma de generación y edición de contenidos audiovisuales.
- Una herramienta para la generación de contenidos para su publicación en portales WEB.
- Una herramienta para el descubrimiento, inventariado y catalogación de activos.
- Una herramienta para la generación de Cuadros de Mando e informes periódicos de seguimiento.
- Una suite SW con las herramientas necesarias para la práctica de análisis forense.

Todas las herramientas las propondrá el adjudicatario y serán suministradas por él y deberán ser aceptadas por MD antes de su configuración y puesta en marcha al servicio de la OGS.

Madrid Digital podrá exigir al adjudicatario, sin coste adicional alguno, la implantación de cualquier otra herramienta, distinta de las anteriores, que a su juicio considere imprescindible para el ejercicio de las funciones de la Oficina o la prestación del servicio de manera óptima. El coste global de esta/s otra/s herramienta/s solicitadas durante el periodo de vigencia del contrato, cuando se trate de software licenciado, no podrá superar, en ningún caso, en valor de mercado, el 5% del importe de adjudicación del contrato por parte del adjudicatario. Estas herramientas no pasarán a ser propiedad de MD a la finalización del servicio.

El adjudicatario deberá mantener permanentemente actualizadas todas las herramientas y plataformas SW de la OGS, asegurando, en todos los casos, las últimas versiones disponibles y los últimos parches de seguridad recomendados por cada fabricante.

---

<sup>1</sup> Documentación sobre proyectos, planes, programas, normativa, informes, resultados de análisis forenses, contenidos de audio y video, planos, esquemas,...etc.





Todo el SW aportado por el adjudicatario deberá cumplir con la normativa de seguridad de MD.

Con carácter general, el adjudicatario deberá observar toda la normativa interna de aplicación para el suministro e instalación del equipamiento en Madrid Digital, como son procedimientos de acceso a los centros, el etiquetado patrimonial de componentes, la normativa técnica de instalación,...etc., que será facilitada al adjudicatario al inicio del contrato.

## CLÁUSULA 5.- MODELO DE GESTIÓN

### 5.1 DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de Madrid Digital, con objeto de garantizar la correcta ejecución de los mismos, y el cumplimiento por tanto de los objetivos del proyecto.

De cara a alcanzar estos objetivos estratégicos, se define una estructura de seguimiento del contrato en dos niveles:

- **Nivel estratégico:** orientado a asegurar la correcta evolución del contrato y la mejora de los servicios, que se encargará de velar por que la estrategia y objetivos de la contratación de servicios estén alineados con los objetivos de Madrid Digital, así como de controlar y garantizar que todas las decisiones y operaciones se ajusten a dicha estrategia.
- **Nivel operativo:** ligado a la ejecución concreta de los servicios, que se encargará de transformar las decisiones estratégicas en planes de acción y de dirigir y controlar los esfuerzos necesarios para su ejecución.

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

- Nivel Estratégico: Comité de Seguimiento del Contrato (**CSC**)
- Nivel Operativo: Comité Técnico y Operativo (**CTO**)

Una vez iniciada la ejecución del contrato, se procederá al nombramiento de ambos Comités, de Seguimiento del Contrato y Técnico y Operativo, que incorporarán personal perteneciente a Madrid Digital y a la empresa adjudicataria.

A los efectos de gobierno del contrato se definen las siguientes figuras por parte de MD:

El **Director del Proyecto** (y, por tanto, responsable último en MD del funcionamiento de la OGS), que será el titular de la Dirección de Seguridad Corporativa (DSC), o persona en quien delegue esta función. En otras partes de este Pliego se le denomina también **Responsable del Contrato** por parte de Madrid Digital.

Los **Jefes del Proyecto**, que serán el titular del Área de Gobierno, Riesgo y Cumplimiento de la Seguridad y Protección de Datos, y el titular del Área de Seguridad Laboral y Régimen Interior, o personas en quien deleguen esta función.

#### 5.1.1 Comité de seguimiento del contrato (CSC).

- El Comité de Seguimiento del Contrato estará formado por las siguientes personas:

Por Madrid Digital:

- El Director del Proyecto de MD
- Los Jefes de Proyecto

Por el adjudicatario:

- El Responsable de la OGS
- El Coordinador de Planes y Proyectos
- El Consultor Senior de Asesoría Jurídica de la OGS, en calidad de Secretario del Comité



Ocasionalmente, el Comité podrá incorporar a sus sesiones al personal asesor o técnico que considere necesario, a juicio de cualquiera de las partes. Ninguna de estas personas figurará como miembro permanente del mismo.

Las funciones de este Comité serán, entre otras, las siguientes:

- Monitorizar el avance global de los servicios.
- Aprobar los cambios propuestos en el seno del Comité Técnico y Operativo que afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o que, por su impacto o importancia estratégica, requieran la aprobación del Comité.
- Controlar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo.
- Acordar la adopción de propuestas de mejora y medidas correctoras o preventivas que deba desarrollar e implantar el adjudicatario, previa autorización de Madrid Digital, en caso de incumplimiento de los ANS o derivadas de planes de mejora.
- Revisar los niveles de servicio inicialmente requeridos, en base a la mejora continua del mismo.
- imprescindibles para la correcta prestación del servicio.
- Determinar el grado de incumplimiento de ANS con el objeto de aplicar las correspondientes penalizaciones que se establecen en el presente Pliego de Prescripciones Técnicas.
- Revisar y analizar las demandas de efectivos al adjudicatario motivadas por la ocurrencia de incidentes graves, servicios especiales o eventos críticos.
- Revisar y aprobar el borrador de factura y resolver cualquier incidencia o problema relacionado con los servicios a facturar en el periodo objeto de revisión.
- Cualquier otro asunto que el propio Comité considere de interés.
- Aprobar ajustes de los ANS definidos en el Pliego y su adaptación a la evolución de los servicios contratados.
- En el caso de que se observase la necesidad de incorporar nuevos servicios de seguridad o componentes que supongan nuevas unidades facturables, y resulten necesarios para la adaptación de la prestación del servicio a las nuevas demandas de seguridad, proponer la modificación de contrato necesaria.

El Comité de Seguimiento del Contrato celebrará sus reuniones en las dependencias de Madrid Digital, con la periodicidad que él mismo determine o, en ausencia de otras indicaciones al respecto, a propuesta del Director del Proyecto.

Se levantará acta de cada una de las reuniones del Comité. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en las *cuarenta y ocho (48)* horas siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma.

### 5.1.2 Comité Técnico y Operativo (CTO).

Su principal objetivo será el seguimiento de la implantación y explotación de los servicios. El Comité Técnico y Operativo estará formado por las siguientes personas:

Por Madrid Digital:

- Los Jefes de Proyecto

Por el adjudicatario:

- El Coordinador de Planes y Proyectos de adjudicatario
- El Consultor Senior de Asesoría Jurídica de la OGS, en calidad de Secretario del Comité

Ocasionalmente, el comité podrá incorporar a sus sesiones al personal asesor o técnico que considere necesario, a juicio de cualquiera de las partes. Ninguna de estas personas figurará como miembro permanente del mismo.

Las funciones de este Comité serán, entre otras, las siguientes:

- Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de los riesgos propios del contrato.
- Garantizar que el personal asignado por el contratista para la ejecución de los servicios está disponible, y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.





- Revisar el estado y evolución de los planes de mejora acordados y cumplimiento de los compromisos aprobados.
- Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los acuerdos de nivel de servicio (ANS) de cada periodo.
- Proponer al CSC, en el caso de que se observase la necesidad de incorporar nuevos servicios de seguridad o componentes que supongan nuevas unidades facturables, y resulten necesarios para la adaptación de la prestación del servicio a las nuevas demandas de seguridad, proponer, si fuera el caso, la modificación de contrato necesaria.
- Analizar y validar, si procede, las propuestas de mejora del servicio efectuadas por el adjudicatario o por MD. En caso de que las propuestas afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o tengan impacto o importancia estratégica, serán elevadas al Comité de Seguimiento del Contrato.
- Revisar y proponer al CSC el borrador de factura y resolver cualquier incidencia o problema relacionado con los servicios a facturar en el periodo objeto de revisión.
- Cualquier otro asunto que el propio Comité considere de interés.

Se levantará acta de cada una de las reuniones del Comité. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en las *cuarenta y ocho (48)* horas siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y a presentación del acta definitiva para la firma.

## 5.2 CONDICIONES GENERALES DE LOS RECURSOS DEL ADJUDICATARIO

Para la correcta prestación de los servicios requeridos se considera imprescindible dedicar a la ejecución del contrato, los recursos humanos mínimos detallados en el apartado **4.5 EQUIPO DE TRABAJO**, siendo responsabilidad del adjudicatario la aportación de los recursos adicionales necesarios para el cumplimiento del pliego y de los acuerdos de nivel de servicio exigidos.

Los empleados del adjudicatario que ejecuten por cuenta de éste trabajos directamente relacionados con el objeto del presente contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por su propia organización, entendiéndose como tal ordenador portátil personal, teléfonos móviles, *tablets*, licencias software ofimático, ...etc.

El licitador deberá aportar, en el **Sobre Nº 1: Documentación Administrativa** documento de compromiso en el que señale, que de resultar adjudicatario del contrato, pondrá a disposición del servicio un equipo de trabajo, con un número de integrantes adecuado para la correcta prestación del servicio objeto del contrato, que cumpla los requerimientos mínimos exigidos, y que cumplirá los requisitos de estabilidad del equipo detallados en el apartado **5.2.1. Condiciones de estabilidad del equipo de trabajo** recogidos en el presente Pliego de Prescripciones Técnicas.

Madrid Digital podrá exigir la ampliación inmediata del número de estos efectivos si no resultaran suficientes para la realización de todas las tareas previstas para la prestación del servicio descrito en este documento.

El licitador que presente la mejor oferta, con carácter previo a la adjudicación del contrato, y en el plazo que le sea requerido, aportará Currículo Vitae de las personas **adscritas al Equipo Base**, propuestas para la ejecución del contrato, siguiendo el modelo definido en el **ANEXO I. MODELO DE CURRÍCULUM**, que detalle sus datos profesionales (categoría profesional, titulación, formación y experiencia), así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

El contratista responderá de la permanente adecuación del personal encargado de la realización de los servicios objeto del contrato. A tal efecto, durante la ejecución de los trabajos, la Agencia podrá comprobar y verificar su capacidad en cualquier momento, pudiendo solicitar la sustitución de los profesionales que considere no idóneos para la prestación del servicio.

La falsedad en el nivel de conocimientos y experiencia de los miembros del equipo asignado por el adjudicatario, así como la sustitución de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y requisitos exigidos en los apartados siguientes, facultará a Madrid Digital para instar la resolución del contrato.



### 5.2.1 Condiciones de estabilidad del equipo de trabajo

Si el contratista propusiera la sustitución de algún componente del equipo de trabajo, deberá comunicarlo por escrito a la Agencia con **quince días naturales** de antelación.

La autorización de cambios ocasionales en la composición del equipo requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de un candidato con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación por el Responsable del Contrato designado por la Agencia de alguno de los candidatos propuestos.

En el supuesto de que se produzcan sustituciones de miembros del equipo adscrito a la ejecución del servicio, se requerirá un solapamiento de los recursos, sin coste adicional para la Agencia, durante un periodo mínimo de **cinco días laborables**.

El incumplimiento de estas obligaciones dará lugar a la aplicación de la correspondiente penalización, según lo indicado en el **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES** de este pliego y en el pliego de cláusulas administrativas.

**El número máximo de sustituciones permitidas será de una persona por semestre.**

### 5.2.2 Modificaciones en la composición del equipo de trabajo a petición de la Agencia

La valoración final de la calidad de los trabajos desarrollados por las personas adscritas a la ejecución del contrato corresponde al Responsable del Contrato designado por la Agencia, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de **siete días naturales**, por otro de igual categoría, si existen razones justificadas que lo aconsejen. El adjudicatario se comprometerá a facilitar la incorporación de los profesionales requeridos en este plazo, desde la comunicación formal por parte de esta Agencia.

Toda nueva incorporación al equipo prestador del servicio deberá cumplir los requisitos mínimos, en cuanto a titulación, formación y actividad profesional establecidos en el presente pliego para cada uno de los recursos.

El incumplimiento de estas obligaciones dará lugar a la aplicación de la correspondiente penalización, según lo indicado en el **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES** de este pliego y en el pliego de cláusulas administrativas.

**Estos cambios propuestos por la Agencia no se tendrán en consideración para el cómputo del número máximo de sustituciones permitidas en el apartado anterior.**

## 5.3 SEGUIMIENTO Y MEJORA CONTINUA DEL SERVICIO

Durante el periodo de ejecución del contrato, el adjudicatario del contrato propondrá las mejoras de calidad que estime oportunas para optimizar la actividad desarrollada. Asimismo, las empresas adjudicatarias habilitarán un **Plan de Seguimiento y Control de Calidad** de los trabajos desempeñados por su personal efectuando, caso de no ser satisfactoria la calidad de los mismos, las medidas correctoras y las horas adicionales que sean necesarias para solventar cualquier incidencia, las cuales correrán por cuenta del adjudicatario, en caso de que las anomalías se debieran a falta de preparación de alguno de los técnicos o a otras causas imputables a la propia empresa.

A tal efecto, los licitadores deberán aportar, en el **Sobre Nº 2**, un **Plan de Calidad**, indicando al menos lo siguiente:

- Cómo se pretende cumplir los niveles de calidad exigidos.
- Cómo se pretenden verificar los cumplimientos.
- Cómo se realimenta el proceso con correcciones en caso de desviaciones de los cumplimientos.



No obstante, durante el desarrollo de los trabajos objeto de contrato, Madrid Digital podrá establecer acciones de seguimiento sobre el control de la calidad y de la actividad desarrollada. En todo caso, el seguimiento y control de la ejecución del contrato se efectuará sobre las siguientes bases:

- Seguimiento continuo de la evolución del proyecto entre el Responsable del Servicio del adjudicatario y el Responsable del Contrato de Madrid Digital o quién éste designe.
- Madrid Digital podrá determinar los procedimientos y herramientas a utilizar para poder llevar cabo la planificación, seguimiento y control del proyecto.
- Seguimiento, mejora y optimización de los servicios prestados.

Así, para el adecuado seguimiento del servicio, evaluación y mejora continua del grado de calidad del mismo se consideran necesarios al menos los siguientes documentos, **a entregar con periodicidad mensual**:

- Informe de seguimiento económico y ANS.
- Informe de seguimiento del servicio.

El incumplimiento de estas obligaciones dará lugar a la aplicación de la correspondiente penalización, según lo indicado en el **ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES** de este pliego y en el pliego de cláusulas administrativas.

#### 5.4 FACTURACIÓN DE LOS SERVICIOS

La facturación se desglosará por tipo según se trate de cuota fija o cuota variable.

Irán con cargo al presupuesto variable del contrato todos aquellos proyectos que el Comité de Seguimiento del Contrato (CSC) defina a lo largo del periodo de vigencia del contrato, y conforme a los servicios expresamente recogidos en este Pliego. La concreción de nuevos proyectos quedará fijada documentalmente por los miembros del CSC. Los nuevos proyectos se detallarán en cuanto a su alcance, valoración económica y facturación en documento aparte, junto al acta de la sesión en la que se hayan aprobado.

Los servicios facturables como cuota variable, es decir, los prestados por efectivos de los denominados equipos de Proyecto o los nuevos proyectos mencionados en el párrafo anterior, podrán solicitarse en cualquier momento, dentro del periodo de vigencia del contrato, según las necesidades de Madrid Digital, en la cantidad que se precise, con la sola limitación del montante económico final del precio de adjudicación global del contrato.

Dentro del presupuesto, la estimación anual realizada de las unidades de cuota variable no implica un compromiso formal de adquisición, sino una estimación de la realidad prevista en la Comunidad de Madrid, a lo largo de la ejecución del contrato.

La liquidación de los servicios con cuota variable será con carácter general a la finalización de los proyectos o encargos, pudiendo el CSC acordar con carácter excepcional la facturación durante los meses en los que efectivamente se preste el servicio.

A continuación se describen los conceptos recogidos y su forma de facturación:

- **Cuota fija:** recoge todos los conceptos por los que se facturará una unidad todos los meses durante la duración del contrato.
- **Cuota variable:** recoge todos los conceptos por los que se facturará con carácter general a la finalización de cada proyecto o encargo por el que efectivamente se preste el servicio.

<b>CLÁUSULA 6.-</b>	<b>CONTENIDO DE LAS OFERTAS</b>
---------------------	---------------------------------

En este capítulo se describe la **estructura y el contenido de la documentación** que debe contener la propuesta técnica que las empresas licitadoras deben presentar y que se incluirá en el **Sobre Nº 2** de la oferta.



Dentro de este sobre no se deberá incluir ninguna información sobre precios, la cual deberá entregarse exclusivamente en el **Sobre Nº 3**, según se especifica en el pliego de cláusulas administrativas.

Resulta obligatorio, para facilitar la valoración de las ofertas, que la documentación presentada en el **Sobre Nº 2**, se ajuste al índice que se especifica en esta cláusula. Los licitadores podrán incluir documentación adicional en anexos si lo consideran necesario. También con carácter obligatorio, la propuesta deberá presentarse en soporte digital compatible con las herramientas instaladas en Madrid Digital.

Adicionalmente, junto a la documentación anteriormente citada los licitadores **podrán adjuntar un resumen ejecutivo** en el que, de forma esquemática y comprensible, recojan el contenido técnico de ese sobre.

En todo caso, cada licitador deberá ajustarse especialmente a lo indicado en este punto, y circunscribir su propuesta exclusivamente a lo demandado en el pliego, separando claramente en la documentación que entregue lo aplicable íntegramente como respuesta tecnológica, evaluable, de la información sobre servicios o productos comerciales que pueda tener en su catálogo comercial, no evaluable.

## 6.1 CONTENIDO DE LAS OFERTAS

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos.

### 6.1.1 Índice.

Definirá los hitos, objetivos y el alcance, así como los aspectos relevantes que se presentan en la oferta.

### 6.1.2 Solución técnica propuesta para los servicios requeridos.

La solución propuesta presentará toda la información concerniente a la metodología de trabajo propuesta, a la planificación detallada de los trabajos a realizar, la organización del equipo de proyecto y a los planes operativos propuestos para la prestación de los servicios requeridos.

#### 6.1.2.1 Planificación, alcance y descripción del proyecto.

Los licitadores deberán presentar un Plan detallado con la información de máximo detalle posible en cuanto a la planificación, estructura y planteamiento o metodología de trabajo propuesto.

#### 6.1.2.2 Plan de implantación de los servicios.

Los licitadores deberán presentar un Plan de Implantación de los servicios, en donde se recojan las distintas fases propuestas del proyecto en base a actividades, procesos y recursos, para la puesta en marcha de los servicios demandados.

El plan de implantación, que en todo caso deberá ser consensuado y aprobado por Madrid Digital al inicio del contrato, deberá recoger al menos los siguientes aspectos:

- Identificación de datos necesarios para el diseño de la OGS, como datos estratégicos y de gobierno de la seguridad, capacidades de seguridad actuales en Madrid Digital o procedimientos operativos vigentes para la gestión de la seguridad.
- Definición de los procesos operativos de la OGS para la gestión de la seguridad, la respuesta a incidentes graves, si fuera necesario, y relaciones con otras áreas de Madrid Digital.
- Organización de la OGS en niveles de servicio, actividades y recursos técnicos.
- Suministro e instalación de las herramientas propuestas para el servicio, tanto de gestión como de operación (gestión documental, desarrollo de contenidos WEB, diseño gráfico, análisis forense,...etc.).
- Desarrollo del portal de gestión.

El Plan de Implantación, detallará claramente para cada fase propuesta el calendario de actividades asociado, plazos estimados y los medios técnicos y humanos dedicados.



La ejecución del Plan de Implantación no deberá superar el plazo de un mes (Fases I y II - Cláusula 11 del presente Pliego) desde el inicio del contrato.

#### **6.1.2.3 Plan de operación y devolución de los servicios.**

En este apartado se describirá el modelo de gestión propuesto para la operación de los servicios, contemplando como mínimo los siguientes aspectos:

- Metodología propuesta para la operación del servicio.
- Propuesta de mecanismos de control y seguimiento del despliegue de proyectos, servicios, herramientas, planes, programas, procesos y marcos de control de la seguridad en MD.
- Propuesta de herramientas para la gestión de la OGS.
- Plan de devolución de servicios que garantice la transferencia de conocimiento, tanto a MD como al nuevo adjudicatario, a la finalización del contrato.

#### **6.1.2.4 Organización del equipo de proyecto.**

Los licitadores deberán presentar la organización de todos los recursos operativos para prestación de todo el servicio.

Deberán realizar un planteamiento con el máximo detalle posible donde se concrete la agrupación de recursos y roles según las capacidades, funciones y servicios a definir y a ejecutar.

Asimismo, deberán concretar la mayor información disponible acerca de la intervención, el rol y la dedicación de cada una de las personas.

#### **6.1.2.5 Plan de Calidad**

Los licitadores deberán presentar un Plan de Calidad y especificar la propuesta de métricas (KPI's y KRI's) e indicadores del servicio así como los mecanismos de obtención y seguimiento de cara a asegurar el cumplimiento de los niveles de calidad del servicio prestado exigidos a lo largo del desarrollo de este pliego, en base a los requisitos especificados en el apartado **5.33 SEGUIMIENTO Y MEJORA CONTINUA DEL SERVICIO**

Se detallará, entre otros, la metodología y procedimientos propuestos por el licitador para el control de los acuerdos de nivel de servicio y penalizaciones asociadas. Se deberá incluir igualmente la propuesta de los informes de seguimiento económico y ANS así como de los de seguimiento del servicio. También se deberá especificar las herramientas concretas que se proponen emplear, cómo propone configurarlas y la información que pretende extraer para su posterior explotación.

#### **6.1.2.6 Plan de capacitación y formación**

El Plan de Capacitación recogerá los programas de los cursos propuestos orientados a la formación sobre los servicios de seguridad objeto del contrato, las herramientas soporte y de gestión propuestas o las metodologías específicas de seguridad aplicadas, entre otros, detallando duración, calendario, periodicidad, contenidos y participantes máximos de cada acción formativa.

Se detallará también la propuesta de contenidos formativos sobre seguridad puestos a disposición de Madrid Digital por el licitador.

### **CLÁUSULA 7.- GESTIÓN DE LA SEGURIDAD**

#### **7.1 Normativa**

Los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se





cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

La Agencia Madrid Digital, en virtud de lo previsto en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de medidas fiscales y administrativas de la Comunidad de Madrid (BOE núm. 52, Jueves 2 marzo 2006) y lo establecido en la citada Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, actuará en calidad de Encargado del Tratamiento de la Comunidad de Madrid en el ámbito de su competencia. Y como Responsable del Tratamiento para aquellos tratamientos así previsto en el registro de actividades de tratamiento ([www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos](http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos)).

## **7.2 Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento**

Para el cumplimiento del objeto de este pliego, el adjudicatario deberá tratar los datos personales de los cuales la Agencia Madrid Digital es Responsable o Encargado del Tratamiento de la manera que se especifica más adelante, en el apartado denominado "Tratamiento de datos personales".

Ello conlleva que el adjudicatario actúe en calidad de Encargado del Tratamiento y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Si el adjudicatario destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerada también como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en el apartado referido al "Tratamiento de Datos Personales", el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que la Agencia Madrid Digital estuviese de acuerdo con lo solicitado emitiría un apartado referido al "Tratamiento de Datos Personales" actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario garantiza el cumplimiento de las siguientes obligaciones, complementadas con lo detallado en el apartado referido al "Tratamiento de Datos Personales":

- a) Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Pliego o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de la Agencia Madrid Digital por escrito en cada momento. El adjudicatario informará inmediatamente a la Agencia Madrid Digital cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.
- b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato.
- c) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes, para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso. En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detallados en el apartado referido al "Tratamiento de Datos Personales".
- d) Mantener absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.
- e) Llevar un listado de personas del equipo prestador del servicio que están autorizadas para tratar los Datos Personales objeto de este pliego, así como los roles asignados a cada una de ellas y la relación de permisos y perfiles autorizados que son estrictamente necesarias para el desempeño de las funciones encomendadas. Garantizar que cada una de las personas del equipo prestador del servicio





se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición de la Agencia Madrid Digital dicha documentación acreditativa.

- f) Garantizar la formación e información necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.
- g) Salvo que cuente en cada caso con la autorización expresa de la Agencia Madrid Digital, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.
- h) Nombrar Delegado de Protección de Datos en caso de que sea necesario según el RGPD, o alternativamente, nombrar Responsable de Seguridad del Servicio del adjudicatario a efectos de protección de los Datos Personales en calidad de responsable del cumplimiento de la regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad. Así como comunicar la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por el adjudicatario.
- i) Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, a devolver (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario por causa del tratamiento; y destruir (iii) los soportes y documentos en que cualquiera de estos datos consten cuando no tengan la consideración de entregable del servicio contratado, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. El Encargado del Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con la Agencia Madrid Digital. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.
- j) Según corresponda, llevar a cabo las instrucciones para el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que se especifiquen, equipamiento que podrá estar bajo el control de la Agencia Madrid Digital o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por la Agencia Madrid Digital, según se establezca en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.
- k) Salvo que se indique otra cosa en el apartado referido al "Tratamiento de Datos Personales" o se instruya así expresamente por la Agencia Madrid Digital, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Pliego o demás documentos contractuales, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito a la Agencia Madrid Digital de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a la Agencia Madrid Digital, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

- l) Con el objeto de dar cumplimiento al artículo 33 RGPD, comunicar a la Agencia para la Administración Digital de la Comunidad de Madrid, de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia



información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.

- m) Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable) ante el Encargado del Tratamiento, éste debe comunicarlo a la Agencia Madrid Digital con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derechos, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho. Asistirá a la Agencia Madrid Digital, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.
- n) Colaborar con la Agencia Madrid Digital en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de riesgos e impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

Asimismo, pondrá a disposición de la Agencia Madrid Digital, a requerimiento de esta, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Pliego y demás documentos contractuales y colaborará en la realización de auditorías e inspecciones llevadas a cabo, en su caso, por la Agencia Madrid Digital.

- o) En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la Agencia Madrid Digital, que contenga, al menos, las circunstancias a que se refiere dicho artículo.
- p) Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de la Agencia Madrid Digital a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición de Agencia Madrid Digital toda información, certificaciones y auditorías realizadas en cada momento.
- q) Derecho de informar: El encargado del tratamiento, en el caso de realizar la recogida de los datos personales, debe facilitar a los interesados la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe aprobar por la Agencia Madrid Digital antes del inicio de la recogida de los datos.

La presente cláusula y las obligaciones en ella establecidas constituyen el contrato de encargo de tratamiento entre la Agencia Madrid Digital y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este pliego y su contrato, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este pliego no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de la Agencia Madrid Digital y que no esté referido en el presente pliego, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el apartado referido al "Tratamiento de Datos Personales". Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales responsabilidad de la Agencia Madrid Digital no contemplados en el apartado referido al "Tratamiento de Datos Personales" el adjudicatario deberá ponerlo en conocimiento de Agencia Madrid Digital, en concreto de su Delegado de Protección de Datos (Dirección de Seguridad Corporativa), con la mayor diligencia y a más tardar en el plazo de 72 horas.



### 7.3 Obligaciones de la Agencia Madrid Digital para la prestación del servicio

- a) Facilitar el acceso del encargado a los datos a los que se refiere el apartado primero del apartado referido al “Tratamiento de Datos Personales”.
- b) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

### 7.4 Sub-encargos de tratamiento asociados a Subcontrataciones

Cuando el pliego permita la subcontratación de actividades objeto del servicio contratado, y en caso de que el adjudicatario pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario lo pondrá en conocimiento previo de la Agencia Madrid Digital, identificando qué tratamiento de datos personales conlleva, para que la Agencia Madrid Digital decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a la Agencia Madrid Digital la decisión de si otorgar, o no, dicho consentimiento):

- a) Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones de la Agencia Madrid Digital.
- b) Que el adjudicatario y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente pliego, el cual será puesto a disposición de la Agencia Madrid Digital a su mera solicitud para verificar su existencia y contenido.

El adjudicatario informará a la Agencia Madrid Digital de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así a la Agencia Madrid Digital la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta de la Agencia Madrid Digital a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

### 7.5 Tratamiento de datos personales

Madrid Digital solo autorizará al adjudicatario a acceder a datos de carácter personal en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, en cuyo caso el adjudicatario asumirá la condición de encargado de tratamiento conforme al artículo 28 del Reglamento General de Protección de Datos, con las obligaciones que lleva aparejadas.

Salvo autorización expresa y por escrito de Madrid Digital, el adjudicatario tendrá prohibido el acceso a los datos personales que se conserven en cada una de las dependencias o sistemas a cuyo interior o contenido deba de acceder. En consecuencia, el adjudicatario habrá de impartir las instrucciones oportunas a su personal para que éste se abstenga de examinar el contenido de los documentos que, en soporte informático, en soporte papel o en cualquier otro tipo de soporte, se encuentre en el interior de las dependencias o sistemas en los que desarrollen sus actividades.

Las actividades de tratamiento a las que pudiera tener acceso el adjudicatario, en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, se encuentran enmarcadas por la norma de la Comunidad de Madrid relativa a las funciones y competencias del Responsable del Tratamiento, así como lo recogido en el Registro de Actividades de Tratamiento publicado en [www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos](http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos).

En concreto, el Encargado de Tratamiento realizará los siguientes tratamientos en el marco de dicha prestación de servicios: Recogida, Registro, Consulta, Modificación, Supresión, Conservación, Transmisión por redes públicas/privadas.

### 7.6 Deber de Información

Los datos de carácter personal del adjudicatario serán tratados por la Agencia Madrid Digital para ser incorporados al sistema de tratamiento “Gestión de los expedientes de adquisición y contratación”, cuya finalidad es la gestión administrativa de los expedientes de contratación de la Agencia y la gestión administrativa de los pedidos a los proveedores de adquisición de bienes y servicios.

Finalidad necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.



Los datos de carácter personal podrán ser comunicados a Unidades Administrativas encargadas de su tramitación, Boletines oficiales, Intervención General o la Cámara de Cuentas.

Se conservarán durante el tiempo que es necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran de dicha finalidad y del tratamiento de los datos.

Los derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, se pueden ejercitar ante la Agencia Madrid Digital, C/Embajadores, 181, 28049 - Madrid o en la dirección de correo electrónico [protecciondatosmadriddigital@madrid.org](mailto:protecciondatosmadriddigital@madrid.org).

Asimismo, los datos del personal del adjudicatario, así como de sus empresas contratistas, si las hubiere, serán tratados por Madrid Digital cuando sea necesario para dar cobertura a la realización de los trabajos objeto del contrato. Su tratamiento quedará incorporado al registro de actividades de tratamiento de la Agencia. Estos datos personales podrán ser comunicados a usuarios y clientes de Madrid Digital cuando así lo requiera la prestación del servicio y se conservarán durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron.

## **Seguridad en la utilización de medios electrónicos**

### **7.7 Normativa**

El adjudicatario está obligado al cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, ENS, (Real Decreto 3/2010 de 8 enero) en lo referido a la adopción de medidas de seguridad de las soluciones tecnológicas o la prestación de servicios ofertados.

El adjudicatario deberá concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

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

### **7.8 Conformidad con el Esquema Nacional de Seguridad**

La Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, determina que cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad según corresponda.

Por ello, Madrid Digital podrá solicitar en todo momento al adjudicatario los correspondientes informes de Autoevaluación o Auditoría, al objeto de verificar la adecuación e idoneidad de lo manifestado en las Declaraciones o Certificados de Conformidad, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de contrato.

## **Medidas de Seguridad**

### **7.9 Documentación de seguridad**

El adjudicatario deberá poseer al inicio de la prestación de los servicios, los siguientes documentos, los cuales deberán estar permanentemente actualizados y a disposición de la Agencia a lo largo de la ejecución del contrato:

- a) Un documento denominado "Política de Seguridad", que estará basada en la Política de Seguridad Corporativa de la Agencia, que consistirá en un documento de alto nivel que defina lo que significa la 'Seguridad de la Información' en la organización y aplicable al servicio prestado. El documento deberá estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible.
- b) Un documento denominado "Documento de Seguridad" coherente con los hitos y medidas de seguridad que se exigen en la presente cláusula y que recoja la información estructurada y ordenada de forma que



describa la relación de las medidas de seguridad propuestas por el adjudicatario para dar respuesta a lo contenido en el presente pliego y que acredite la forma en la que se procederá al cumplimiento de las mismas. Asimismo, deberá, identificar las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio y del Delegado de Protección de Datos del adjudicatario.

#### **7.10 Confidencialidad y deber de secreto**

El adjudicatario se compromete de forma específica a tratar como confidencial toda aquella información responsabilidad de Madrid Digital a la que pueda tener acceso, con motivo de la prestación de sus servicios y se compromete a que dichos datos permanezcan secretos incluso después de finalizado el presente Acuerdo.

Debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.

A estos efectos, el adjudicatario se compromete a tomar, respecto de sus empleados o colaboradores, las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como encargado de tratamiento y que, en consecuencia, deben respetar, así como a garantizar que los datos personales que conozcan en virtud de la prestación del servicio permanecen secretos incluso después de finalizado el presente Acuerdo por cualquier causa.

Dicha obligación de información a los empleados y colaboradores del adjudicatario se llevará a cabo de modo tal que permita la documentación y puesta a disposición de la Agencia Madrid Digital del cumplimiento de aquella obligación.

#### **CLÁUSULA 8.- PROPIEDAD DE LOS TRABAJOS**

Todos los informes, estudios y documentos, elaborados por los contratistas como consecuencia de la ejecución de los contratos 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.

Los adjudicatarios renuncian expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución de los contratos 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 Madrid Digital.

#### **CLÁUSULA 9.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS**

Los contratistas no adquieren 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.

Los contratistas no podrán utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato, y no podrán transmitirla sin el consentimiento expreso y escrito de Madrid Digital.

Finalizado el presente contrato, los desarrollos software, herramientas y licencias incluidas en el alcance de los servicios del presente pliego pasarán a ser propiedad de Madrid Digital, de acuerdo con lo indicado en la cláusula 4.7 TECNOLOGÍAS Y HERRAMIENTAS del presente documento

#### **CLÁUSULA 10.- CALIDAD DEL SERVICIO**

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, Madrid Digital podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.





**CLÁUSULA 11.- PLAZO, DURACIÓN Y ETAPAS DE PRESTACIÓN DE LOS SERVICIOS**

El plazo de ejecución del contrato será de **24 MESES**, desde el 1 de octubre de 2019 hasta el 30 de septiembre de 2021.

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, Madrid Digital quedará facultada para instar la resolución del contrato.

Durante el periodo final de vigencia del contrato o, en su caso, en cualquiera de sus prórrogas, Madrid Digital establecerá un periodo transitorio de ejecución en condiciones especiales, de modo que se garantice la prestación del servicio de forma ininterrumpida, comprometiéndose el adjudicatario a colaborar con el nuevo adjudicatario en aquellas actividades necesarias, encaminadas a la planificación y ejecución del cambio. Concretamente, durante este periodo que durará **dos meses**, correrá por cuenta del adjudicatario de este contrato, como mínimo, lo siguiente:

- La plena integración de las plataformas SW del servicio con las que MD determine, de su propiedad.
- La formación y transferencia de conocimiento y documentación del servicio al personal de MD y al equipo del nuevo adjudicatario.
- El volcado de información y de contenidos a las plataformas de MD así como a las del nuevo adjudicatario.
- La generación de informes finales del servicio.

Y cualquier otra actividad que MD determine con el fin de asegurar la continuidad del servicio de la OGS en óptimas condiciones.

Además de lo anterior, el adjudicatario del contrato se compromete a garantizar la completa y correcta operatividad de todos los servicios durante el periodo de transición requerido a la finalización del contrato.

La prestación del servicio se llevará a cabo en base a las siguientes **seis (6) fases** o etapas:

- **FASE I: Establecimiento de la OGS (duración: 15 días).** Presentación y difusión en MD de las competencias de la OGS para el soporte a la gestión y al gobierno de la seguridad. Conformación del equipo humano y asignación de los recursos para el desempeño de sus funciones básicas.
- **FASE II: Identificación de las unidades operativas (duración: 15 días).** A partir de la primera planificación para la implantación de las funciones de la Oficina, identificación de las unidades operativas de MD especializadas en los ámbitos de seguridad afectados por el despliegue de las capacidades, programas, procesos y marcos de control definidos en la Estrategia de Ciberseguridad de la Agencia.
- **FASE III: Definición y establecimiento de comités (duración: 15 días) y planificación del primer despliegue de programas y servicios.** Definición y constitución de los comités necesarios para la coordinación con las UO encargadas del primer despliegue de los servicios, procesos y marcos de control definidos en la Estrategia de Seguridad de MD.
- **FASE IV: Despliegue inicial de capacidades, funciones y servicios de la OGS (duración: 75 días).** Siguiendo las directrices y la planificación de MD, despliegue del primer conjunto de servicios y programas en base a una dotación parcial de los recursos previstos para la Oficina. Seguimiento y medida de resultados, y reporte a la Dirección de MD. Valoración de recursos definitivos, planificación de las siguientes etapas y crecimiento planificado del equipo de la Oficina.
- **FASE V: Despliegue programado de capacidades y servicios (duración: 20 meses).** Despliegue completo de capacidades, servicios y programas a gestionar por la OGS en base a la programación establecida por MD. Constitución plena de las capacidades de la Oficina y de su equipo de trabajo.
- **FASE VI: Entrega de los servicios al nuevo adjudicatario (duración: Los dos (2) últimos meses de contrato / junto a Fase V).** Entrega de los servicios al nuevo adjudicatario: Integración de plataformas, volcado de contenidos, formación al nuevo adjudicatario y al personal de MD, generación de informes finales...etc., sin detrimento del servicio ordinario que venga prestando la Oficina.





	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
	Q	Q	Q	Q	Q	Q	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
■ FASE I: (duración: 15 días)																								
■ FASE II: (duración: 15 días)																								
■ FASE III: (duración: 15 días)																								
■ FASE IV: (duración: 75 días)																								
■ FASE V: (duración: 20 meses)																								
■ FASE VI: (duración: 2 meses)																								

## CLÁUSULA 12.- GARANTÍA DE LOS TRABAJOS

Se establece un plazo de garantía de **DOCE 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, cada adjudicatario responderá de la correcta realización de los trabajos que se le hayan contratados, de los equipamientos instalados 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 13.- CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente Pliego de Prescripciones Técnicas, el licitador podrá dirigirse a:

Agencia para la Administración Digital de la Comunidad de Madrid  
Subdirección General de Recursos  
Dirección de Seguridad Corporativa

E-mail: DSC@MADRID.ORG

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con Madrid Digital, para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Por su parte la Agencia se compromete a responder en los términos indicados en la Cláusula 10 del Pliego de Cláusulas Administrativas Particulares.

*El Director de Seguridad Corporativa*

*Fdo.: Fernando Ledrado Gómez*



**ANEXO I. MODELO DE CURRÍCULUM**

**MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO**

**(A aportar para cada miembro del equipo propuesto)**

<b>APELLIDOS:</b>	
<b>NOMBRE:</b>	
<b>CATEGORÍA PROFESIONAL:</b>	
<b>TTITULACIÓN / UNIVERSIDAD o CENTRO / HOMOLOGACIÓN (en caso de haberse obtenido la titulación fuera de España):</b>	
<b>FORMACIÓN:</b>	
<b>ACTIVIDAD PROFESIONAL (Especificando como mínimo: Empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta):</b>	

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

- **FIN DEL ANEXO I** -



**ANEXO II. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**

SERVICIO	REQUISITO	NIVEL DE SERVICIO EXIGIDO	PENALIZACIÓN
Constitución de la OGS: Disponibilidad de todos los efectivos humanos y perfiles profesionales según especificaciones del PPT	Implantación del servicio	T. Máximo = 1 día natural a contar desde la fecha de inicio de contrato	2.000 € por cada día natural de retraso
Entrega de servicios y proyectos	Entrega de servicios / proyectos con la calidad requerida y en el plazo acordado entre el Coordinador de Planes y Programas y el Jefe de Proyecto de MD	En la fecha comprometida entre el Coordinador de Planes y Programas y el Jefe de Proyecto de MD	3.000 € por cada día natural de retraso
Entrega de documentos, informes, contenidos audiovisuales y otros entregables derivados de la actividad de la OGS	Entrega de documentos y contenidos con la calidad requerida y en el plazo acordado entre el Coordinador de Planes y Programas y el Jefe de Proyecto de MD	En la fecha comprometida entre el Coordinador de Planes y Programas y el Jefe de Proyecto de MD	500 € por cada día natural de retraso y por cada entregable identificable separadamente
Servicios / proyectos a desempeñar por efectivos del Equipo Proyectos	Disponibilidad del número de efectivos requerido con el perfil solicitado en base al servicio / proyecto previamente definido	T. Máximo = 7 días, para cualquier perfil	3.000 € por cada día de retraso y por cada perfil
Atención a consultas, peticiones o llamadas	Tiempo máximo de respuesta	T. Máximo = 1 día	500 € por cada día de retraso
Atención a consultas, peticiones o llamadas	Tiempo máximo de resolución definitiva o parcial a una consulta, petición o llamada	T. Máximo = 3 días	500 € por cada día de retraso
Operatividad de las herramientas SW de gestión de la OGS. Dotación mínima según apartado 4.7 TECNOLOGÍAS Y HERRAMIENTAS del PPT	Implantación, parametrización y plena operatividad de todos los sistemas	T. Máximo = 15 días	2.000 € por cada día natural de retraso y por cada herramienta
Entrega de informes mensuales	Tiempo de entrega de informes mensuales del Servicio y de Seguimiento económico y ANS. (Apartado 5.3 del PPT)	Quinto (5º) día hábil del mes siguiente.	1.000 € por cada día natural de retraso
Asesoría legal	Tiempo de entrega de informes de asesoría legal	T. Máximo = 7 días naturales	1.000 € por cada día natural de retraso



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: **1019629385769945216829**

Peritaje forense	Tiempo de entrega de informes periciales forenses	T. Máximo = 15 días naturales	1.000 € por cada día natural de retraso
Personal adscrito a los equipos	Disponibilidad de sustituto por detección de incumplimiento de perfil exigido	T. Máximo a emplear en la sustitución = 7 días naturales.	2.000 € por cada día natural de retraso en cada sustitución solicitada
Personal adscrito a los equipos	Periodo mínimo de solapamiento entre efectivos	T. mínimo de solapamiento = 5 días laborables.	5.000 € por cada día natural de carencia en el programa de 5 días de solapamiento
Personal adscrito a los equipos	Nº Máximo de sustituciones permitidas por tipo de perfil	1 cambio semestral	10.000 € por cada cambio adicional
Tratamiento de incidentes de seguridad graves	Disponibilidad de perfiles profesionales cualificados y medios técnicos por parte del adjudicatario	T. Máximo = 4 horas desde la comunicación formal del incidente grave al adjudicatario.	1.000 € por cada hora de retraso en cualquiera de los perfiles solicitados
Operatividad de las herramientas SW de gestión de la OGS. Dotación mínima según apartado 4.7 TECNOLOGÍAS Y HERRAMIENTAS del PPT	Disponibilidad de cada sistema	Disponibilidad ≥ 95%	1.000 € por indisponibilidad

Para todos aquellos ANS asociados al cálculo de disponibilidad, ésta se calculará, por periodos de 1 mes desde la última indisponibilidad no penalizada, aplicando la siguiente fórmula:

$$D = \frac{T_{tot} - T_{nodisp}}{T_{tot}} * 100 (\%)$$

Dónde:

D = disponibilidad

T<sub>tot</sub> = tiempo total del periodo considerado (en minutos).

T<sub>nodisp</sub> = tiempo de no disponibilidad del servicio dentro del intervalo T<sub>tot</sub> considerado (en minutos).

No se computarán los tiempos de mantenimiento programado debidamente comunicados y autorizados por Madrid Digital dentro del periodo de cálculo.

- FIN DEL ANEXO II -

