

Pliego de Prescripciones Técnicas

***“SERVICIOS DE GOBIERNO, RIESGO Y CUMPLIMIENTO
DE SEGURIDAD DE LA INFORMACIÓN DE MADRID
DIGITAL (3 LOTES)”***



**PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL CONTRATO DE SERVICIOS DENOMINADO
“SERVICIOS DE GOBIERNO, RIESGO Y CUMPLIMIENTO DE SEGURIDAD DE LA
INFORMACIÓN DE MADRID DIGITAL (3 LOTES)” A ADJUDICAR MEDIANTE
PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS.**

ÍNDICE

CLÁUSULA 1. INTRODUCCIÓN	3
CLÁUSULA 2. OBJETO, ÁMBITO Y ALCANCE.....	4
CLÁUSULA 3. CONSIDERACIONES GENERALES	5
CLÁUSULA 4. LOTE 1: SERVICIOS DE LA OFICINA DE GOBIERNO DE SEGURIDAD (OGS).....	7
4.1 Ámbito de GOBIERNO:	7
4.2 Ámbito de PREVENCIÓN:.....	15
4.3 Ámbito de DETECCIÓN:	18
4.4 SERVICIOS DE CUOTA FIJA Y VARIABLE.....	19
CLÁUSULA 5. LOTE 2: SERVICIOS DE AUDITORÍA Y VERIFICACIÓN DE CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN.	19
5.1 Ámbito de DETECCIÓN:	20
CLÁUSULA 6. LOTE 3: SERVICIOS DE AUDITORÍA DE CERTIFICACIÓN DE CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN. (CUOTA VARIABLE)	24
6.1 Ámbito de PREVENCIÓN:.....	25
6.2 Ámbito de DETECCIÓN:	25
CLÁUSULA 7. EQUIPO DE TRABAJO	26
7.1 LOTE 1: Servicios de la Oficina de Gobierno de Seguridad (OGS).....	26
7.2 LOTE 2: Servicios de auditoría y verificación de cumplimiento de seguridad de la información.....	40
7.3 LOTE 3: Servicios de auditoría de certificación de cumplimiento de normas de seguridad de la información	45
7.4 TECNOLOGÍAS Y HERRAMIENTAS	46
CLÁUSULA 8. MODELO DE GESTIÓN.....	47
8.1 HORARIO Y LUGAR DE PRESTACIÓN DE LOS SERVICIOS	47
8.2 DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS	47
8.3 CONDICIONES GENERALES DE LOS RECURSOS DEL ADJUDICATARIO	53
CLÁUSULA 9. FORMACIÓN PARA EMPLEADOS DE MADRID DIGITAL	56
CLÁUSULA 10. CALIDAD DEL SERVICIO	57
CLÁUSULA 11. PLAZO, DURACIÓN Y ETAPAS DE PRESTACIÓN DE LOS SERVICIOS	57
CLÁUSULA 12. CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS	59
ANEXO I. MODELO DE CURRÍCULUM.....	60
ANEXO II. ACUERDOS DE NIVEL DE SERVICIO	61

CLÁUSULA 1. INTRODUCCIÓN

De acuerdo con lo establecido en el *Artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 30 de diciembre de 2005), 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), por la *Ley 11/2022, de 21 de diciembre, de Medidas Urgentes para el Impulso de la Actividad Económica y la Modernización de la Administración de la Comunidad de Madrid –artículo 26–* (B.O.C.M. núm. 304, de 22 de diciembre de 2022), y por el *Artículo 7 de la Ley 8/2024, de 26 de diciembre, de medidas para la mejora de la gestión pública en el ámbito local y autonómico de la Comunidad de Madrid* (BOCM número 308, de 27 de diciembre de 2024), la **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante la **Agencia**), se configura como ente público de los previstos en el *Artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid*, con personalidad jurídica propia, plena capacidad jurídica y de obrar para el cumplimiento de sus fines y con plena autonomía orgánica y funcional, que tiene por objeto, de acuerdo con las directrices establecidas por la consejería competente en materia de Digitalización, la planificación y ejecución de proyectos y servicios relacionados con tecnologías de la información, comunicaciones electrónicas y ciberseguridad, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información, en el ámbito de actuación definido en el apartado dos de este artículo 10.

Entre las competencias que, conforme al *Artículo 10 – Tres de la Ley 7/2005, de 23 de diciembre*, se atribuyen a la Agencia, bajo la dirección y coordinación de la Consejería competente en materia de Digitalización, para el cumplimiento de sus objetivos, se recogen, en concreto, las siguientes:

- a) *La planificación, desarrollo y ejecución de planes y proyectos de tecnología, de comunicación electrónica y de seguridad de la información de la administración General e Institucional de la Comunidad de Madrid, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información.*
- d) *La adquisición, el diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica, sistemas de información y de comunicaciones electrónicas y seguridad de la información de titularidad de la Agencia, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento, los centros de procesos de datos, incluido el uso de nubes públicas y privadas de la Comunidad de Madrid y el archivo electrónico único de los expedientes y documentos electrónicos.*
- i) *El desarrollo, implantación, mantenimiento, gestión y evolución del modelo de gobernanza tecnológica que proporcione el catálogo de servicios y métricas asociadas, con seguimiento estandarizado de acuerdos de nivel de servicio, así como un cuadro de mandos del gasto en materia de tecnologías y comunicaciones.*

El desarrollo de estas competencias de seguridad de la información y ciberseguridad es uno de los cinco objetivos del Plan Estratégico 2022-26 de Madrid Digital, cuyo propósito es: *Hacer de la Comunidad de Madrid una Administración más segura, confiable y resiliente.*

Este objetivo se desarrolla en dicho plan a través de cuatro medidas estratégicas o líneas de actuación, dos de ellas dedicadas al **gobierno, riesgo y cumplimiento de seguridad de la información** (en adelante, GRCSI) y a la concienciación del personal en materia de seguridad.

En consecuencia, con esta contratación se pretende:

- Promover la mejora la gestión y mejora continua de la seguridad en Madrid Digital aplicando los principios básicos del Esquema Nacional de Seguridad, especialmente la visión y entendimiento de la seguridad como un proceso integral y asumiendo la gestión de la seguridad con un enfoque basado en los riesgos.
- Aumentar y mejorar las capacidades humanas, organizativas y tecnológicas en materia de seguridad de los ámbitos de gobierno, prevención y detección asociadas al gobierno, riesgo y cumplimiento de seguridad de la información (GRCSI).
- Disponer y desarrollar las capacidades necesarias ante las numerosas normativas legales y de buenas prácticas de seguridad que afectan a Madrid Digital y las obligaciones y consecuencias que ello acarrea.
- Disponer de más flexibilidad y capacidad en la identificación de los riesgos de cumplimiento de las normativas de seguridad de la información a las que Madrid Digital debe dar respuesta.
- Aumentar la madurez de las capacidades de seguridad ya existentes en Madrid Digital en los ámbitos de gobierno, prevención y detección en lo que se refiere al GRCSI de la Agencia.
- Reforzar las capacidades de detección de seguridad de la información mediante la realización de auditorías de cumplimiento de seguridad de la información.
- Dar cumplimiento a la obligación de Madrid Digital respecto de la realización periódica de auditorías de seguridad de la información y de facilitar el reporte del estado de la seguridad a los distintos reguladores estatales en esta materia.
- Continuar y seguir impulsando la obtención de la certificación de cumplimiento de las normativas UNE-EN ISO/IEC 27001:2023 y Esquema Nacional de Seguridad en los distintos servicios de Madrid Digital.
- Promover e inculcar una cultura de concienciación de seguridad de la información entre todo el personal de la Comunidad de Madrid y, en especial, entre el personal de Madrid Digital.

Ante la necesidad de garantizar la continuidad y cobertura de las necesidades descritas, y siendo competencia de la Agencia proporcionar el servicio que se pretende, atendiendo a la especificidad de los servicios que constituyen su objeto, y la necesidad de abordar los mismos de manera eficaz y con las garantías requeridas, procede la tramitación del oportuno expediente de contratación.

CLÁUSULA 2. OBJETO, ÁMBITO Y ALCANCE

El objeto del presente contrato es la prestación de los servicios de **gobierno, riesgo y cumplimiento de seguridad de la información** que son necesarios para dotar a la Agencia de determinadas capacidades, funciones y servicios de ciberseguridad contemplados en el propio modelo funcional y organizativo de ciberseguridad de Madrid Digital, de conformidad con lo establecido en el presente Pliego de prescripciones técnicas.

Se divide en los siguientes lotes:

- **LOTE 1:** Servicios de la Oficina de Gobierno de Seguridad (OGS-Madrid Digital).
- **LOTE 2:** Servicios de Auditoría y verificación de cumplimiento de las normativas, estándares y buenas prácticas de seguridad de la información aplicables en Madrid Digital (AUD-Madrid Digital).
- **LOTE 3:** Servicio de certificación y acreditación de cumplimiento de las normativas, estándares y buenas prácticas de seguridad de la información aplicables en Madrid Digital (CERT-Madrid Digital).

El **ámbito de actuación** de los servicios descritos en este documento se circunscribe a los sistemas, servicios e infraestructuras TIC de Madrid Digital y que intervienen en el ejercicio de las competencias que tiene asignadas.

El **alcance** de los trabajos se determina en desarrollo específico de cada uno de los lotes en los que se estructura el presente pliego.

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 de seguridad interna aplicable en Madrid Digital, así como a incorporarla y tenerla en cuenta durante la ejecución del contrato. Ejemplos de este punto son la política de seguridad de la información, el documento marco de competencias de las figuras, roles y responsabilidades en la organización de la seguridad de Madrid Digital, las políticas de control de acceso y gestión de recursos vigentes, las normativas de seguridad y los procedimientos operativos relacionados con la seguridad 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 presente Pliego de Prescripciones técnicas.

El adjudicatario de cada uno de los lotes dispondrá de manera autosuficiente de los recursos técnicos, humanos, logísticos y materiales necesarios para proporcionar asistencia y soporte a Madrid Digital (Madrid Digital) en todos y cada uno de los ámbitos, funciones, capacidades y servicios que se enumeran a continuación.

Madrid Digital estima que para dotar los equipos de trabajo de cada lote son necesarios, como mínimo, los perfiles profesionales y los efectivos humanos que se describen en la cláusula 7 de este pliego “**EQUIPO DE TRABAJO**”.

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 Madrid Digital.

El adjudicatario aportará, especialmente, personal de apoyo y soporte siempre que sea preciso cumplir objetivos de calidad y plazos de entrega comprometidos por la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad con Madrid Digital (en adelante SGCPDP) o desde Madrid Digital hacia la Comunidad de Madrid, cuando estos servicios o proyectos tengan relación con los servicios incluidos en este pliego. Estos recursos, en caso de ser necesarios, no supondrán sobre coste alguno para Madrid Digital.

El responsable de GRCSI de Madrid Digital 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 los adjudicatarios.

El adjudicatario aportará por su cuenta al contrato las herramientas necesarias para la prestación del servicio (Apartado **7.4 TECNOLOGÍAS Y HERRAMIENTAS**).

El adjudicatario empleará únicamente formatos y soportes lógicos o físicos para la gestión de la información compatibles con los homologados por Madrid Digital.

En lo referente a los ámbitos de actuación sobre los que se prestarán los servicios relativos a los tres lotes mencionados se tendrá como referencia lo establecido en el **modelo de ciberseguridad de Madrid Digital**, que se organiza en **cuatro ámbitos**:

1. **Gobierno**
2. **Prevención**
3. **Detección**
4. **Recuperación y Respuesta**

Para cada uno de estos ámbitos, agrupadas por dominios de seguridad, se propone la relación de las capacidades de ciberseguridad que Madrid Digital debe adquirir y desarrollar, así como los diferentes servicios y actividades de seguridad incluidos en cada una de ellas.

Por otra parte, la SGCPDP tiene asignadas, dentro de Madrid Digital, determinadas competencias orientadas a alcanzar los objetivos de seguridad de la información marcados por el Comité de Dirección de la Agencia y el cumplimiento de la legislación o normativa de aplicación en materia de seguridad de la información.

Una parte de esas competencias están referidas al GRCSI y se concretan en:

- Gestionar la estrategia y gobierno de la ciberseguridad y protección de datos.
- Gestionar las relaciones externas en materia de ciberseguridad.
- Gestionar los planes y programas de ciberseguridad y seguridad en materia de protección de datos.
- Realizar el análisis de riesgos de ciberseguridad.
- Gestionar las auditorías de ciberseguridad y protección de datos.
- Gestionar la formación y concienciación en materia de ciberseguridad y protección de datos.

Cada una de estas competencias se materializan, para cada ámbito y dominio de seguridad, adquiriendo y mejorando la madurez de las distintas capacidades del modelo de ciberseguridad de Madrid Digital y, para cada una de ellas, el desarrollo y prestación de los diferentes servicios y actividades de seguridad que correspondan.

CLÁUSULA 4. LOTE 1: SERVICIOS DE LA OFICINA DE GOBIERNO DE SEGURIDAD (OGS).

La actividad de la **Oficina de Gobierno de la Seguridad (OGS)** se centrará en la adquisición, mejora y desarrollo de aquellas capacidades de seguridad de los **ámbitos de gobierno, prevención y detección** y de sus líneas de servicio asociadas, que tienen por objeto el ejercicio de las competencias de la SGCPDP en materia de GRCSI.

La **OGS** llevará a cabo, bajo la dirección de Madrid Digital, las siguientes actividades:

4.1 Ámbito de GOBIERNO:

4.1.1 Dominio: Estrategia y gobierno de la ciberseguridad

4.1.1.1 Capacidad: Apoyo a la Dirección en la definición de la estrategia de ciberseguridad

Servicios y actividades a realizar:

- Revisión del diseño y la organización de los procesos de GRCSI:
 - Estudiar las competencias de la SGCPDP asignadas en el ámbito de GRCSI.
 - Analizar las capacidades de seguridad y las distintas líneas de servicio en el ámbito de GRCSI que se han identificado en el modelo de ciberseguridad de Madrid Digital.
 - Reorganizar para cada competencia: las capacidades y líneas de servicio que correspondan en cada caso.
 - Proponer un modelo de ficha de línea de servicio, incluyendo, como mínimo, el objetivo de la misma, la descripción de las tareas a realizar, así como cualquier otra información que se considere necesaria y documentar todas las fichas en consecuencia.
 - Identificar y documentar el flujo de información e interacciones entre las distintas líneas de servicio y sus tareas asociadas.
 - Definir y diseñar el modelo de automatización de las líneas de servicio GRCSI, a través de la ejecución de las diferentes tareas a realizar en cada una de ellas, identificando y documentando los diferentes casos de uso de tareas de GRCSI automatizadas.
 - Proponer la arquitectura y las herramientas necesarias o más adecuadas, en entornos colaborativos de Microsoft 365 y de Microsoft Power Platform, para implantar el modelo de automatizado de líneas de servicio y tareas GRCSI.
 - Implantar el modelo propuesto de automatización de cada una de las líneas de servicio y sus tareas GRCSI del modelo propuesto.

4.1.1.2 Capacidad: Identificación de la normativa de seguridad de la información aplicable a MD

Servicios y actividades a realizar:

- Identificación de la normativa de seguridad de la información aplicable a MD y definición el alcance de la misma.
 - Identificar toda la legislación/regulación vigente o en desarrollo normativo, de aplicación en el ámbito de Seguridad de la Información, que sea de obligado cumplimiento por MD y/o por las Consejerías de la Comunidad de Madrid.

- Identificar códigos de buenas prácticas, de cumplimiento opcional en MD, orientándolas y aplicándolas al ámbito de negocio o de operación correspondiente de MD.
- Identificar, para cada legislación o normativa de obligado cumplimiento y/o buenas prácticas, los documentos normativos de seguridad necesarios para dar cumplimiento a las anteriores y determinar su existencia en el cuerpo normativo de seguridad de MD.
- Elaborar y mantener un inventario completo de las normativas y buenas prácticas de seguridad aplicables, así como de la normativa interna de seguridad de MD.

4.1.1.3 Capacidad: Elaboración y mantenimiento del Cuadro de Mando de GRCSI.

Servicios y actividades a realizar:

- Propuesta y elaboración del diseño del Cuadro de Mando GRCSI.
 - Identificar la información relevante de cada una de las capacidades de GRC de Seguridad, el origen de la misma y sus indicadores correspondientes, para realizar un seguimiento de la misma y facilitar la toma de decisiones.
 - Analizar los indicadores y métricas existentes en las distintas capacidades GRC, definir aquellas otras que sean necesarias para completar y tener una visión completa de estado de situación del ámbito de GRC de seguridad en MD.
 - Realizar un prototipo de cuadro de mando para verificar la idoneidad de la información analizada y de la medición realizada.
 - Realizar el diseño técnico del propio cuadro de mando y construirlo sobre las herramientas de O365 que MD estime adecuadas.
- Medición periódica de los indicadores y reporte del estado del GRCSI.
 - Recabar la información de los indicadores definidos.
 - Generar el reporte del estado de la medición, con informes de resultados y analizar su contenido para obtener conclusiones y propuestas de mejora.
 - Realizar cuanta documentación sea necesaria para ampliar o matizar los informes de resultados.

4.1.1.4 Capacidad: Reporte a Órganos Internos y representación GRC en el Comité de Dirección de Seguridad de la información de MD

Servicios y actividades a realizar:

- Reporte al Comité de Dirección de Seguridad de la información de MD.
 - Analizar las actuaciones de seguridad más relevantes realizadas en MD durante el último periodo y preparar la información y la documentación ejecutiva correspondiente.
 - Preparar la documentación necesaria para realizar propuestas de actuaciones en materia de seguridad que requieran de la aprobación y del patrocinio del propio Comité.
- Reporte a la Subdirección General de Ciberseguridad.
 - Elaborar la documentación y extraer la información de los indicadores más relevantes que deberán de ser reportados a la Subdirección General de Ciberseguridad.

- Dar soporte en la elaboración de la propuesta de la agenda del Comité de Dirección de Seguridad en materia de Gobierno, Riesgo y Cumplimiento de Seguridad de la Información.
- Elaborar la documentación necesaria para presentar los resultados del Informe anual de estado y propuesta de mejora de la Seguridad de la Información de MD.
- Elaborar la documentación necesaria para presentar el Plan Anual de Auditoría de cumplimiento de seguridad de MD.
- Elaborar la documentación necesaria para presentar el Plan de certificación de cumplimiento de los servicios de MD en las normas UNE-EN ISO/IEC 27001:2023 y ENS.

4.1.2 Dominio: Relaciones externas en materia de ciberseguridad.

4.1.2.1 Capacidad: Reporte y comunicación con Reguladores y Organismos externos en materia GRC de seguridad

Servicios y actividades a realizar:

- Reporte y comunicación con reguladores gubernamentales en materia de GRCSI.
 - Dar soporte en la elaboración de documentación y extracción de información requerida periódicamente por los propios Organismos reguladores de seguridad: CCN, CNPIC, OCC, etc.
 - Dar soporte en el análisis de las peticiones recibidas, en materia de GRCSI, por los Organismos reguladores de seguridad y en la preparación de la información necesaria para dar respuesta a las mismas.
 - Colaborar con las distintas unidades organizativas de MD en el análisis y respuesta de peticiones de información por parte de Cuerpos y Fuerzas de Seguridad del Estado.
- Reporte y comunicación con órganos de la CM
 - Dar soporte en el análisis de las peticiones recibidas, en materia de GRC de seguridad, por los distintos Órganos de la Comunidad de Madrid y en la preparación de la información necesaria para dar respuesta a las mismas.

4.1.3 Dominio: Cumplimiento de la legislación y normativa de seguridad de la información.

4.1.3.1 Capacidad: Adecuación y cumplimiento del Esquema Nacional de Seguridad, en el ámbito de los servicios de MD

Servicios y actividades a realizar:

- Elaboración y actualización de los criterios de categorización de los sistemas ENS de MD, que incluya los referentes a la valoración de la información y del servicio en cada una de las dimensiones que corresponda.
- Soporte a los distintos responsables de MD en la caracterización de cada uno de los sistemas ENS de MD:
 - Caracterizar los activos que conforman cada uno de los sistemas ENS de MD.
 - Interpretar y aplicar los criterios para determinar la valoración de los activos esenciales (información y servicios) de cada uno de los sistemas ENS de MD.

- Obtención de la categorización de los sistemas ENS de MD y generación de los informes para formalizarlo por el Responsable correspondiente de MD.
- Generación de la declaración de aplicabilidad provisional:
 - Determinar las medidas de seguridad aplicables atendiendo a los resultados de la categorización del sistema ENS y de la valoración de los activos esenciales.
- Valoración de la madurez de la seguridad del sistema ENS:
 - Identificar, junto con el responsable del sistema, aquellas medidas de seguridad de la declaración de aplicabilidad provisional que no aplican finalmente en la seguridad del sistema ENS.
 - Determinar, junto con el responsable del sistema, el nivel de madurez de cada una de las medidas de seguridad que aplican finalmente en la seguridad del sistema ENS.
 - Generar el informe de declaración de aplicabilidad definitiva con la valoración final de seguridad realizada y realizar la propuesta de su firma por parte del Responsable de Seguridad de MD.

4.1.3.2 Capacidad: Adecuación y cumplimiento de normativas de seguridad, en el ámbito de los servicios esenciales o servicios críticos de MD

Servicios y actividades a realizar:

- Soporte a los distintos responsables de MD en el análisis y determinación de la criticidad de los servicios de MD y caracterización de los activos que conforman cada uno de ellos.
- Elaboración y actualización de la documentación correspondiente a las políticas, planes, programas, metodologías o documentación complementaria que se requiera o se precise desarrollar para dar cumplimiento en MD a cualquier legislación o normativa que pudiera estar relacionada con los servicios de MD de tipo crítico o esencial.

4.1.3.3 Capacidad: Adecuación y cumplimiento de la UNE-EN ISO/IEC 27001:2023 en el ámbito de los servicios de MD

Servicios y actividades a realizar:

- Mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información (SGSI) de los servicios prestados por MD.
 - Analizar periódicamente el alcance del SGSI y valorar su idoneidad.
 - Revisar y actualizar la documentación existente del SGSI. En caso necesario, elaborar la documentación que sea necesaria para complementar la existente.
 - Realizar el seguimiento de la consecución de los objetivos del SGSI, que se plantean anualmente.
 - Establecer los criterios de medición de la eficacia del SGSI.
 - Proponer las acciones correctoras o de mejora del SGSI y realizar seguimiento de la consecución de las mismas.
 - Elaborar la documentación necesaria para proponer a la Dirección de MD la revisión del SGSI de forma periódica.

4.1.3.4 Capacidad: Soporte en el cumplimiento de las normativas de seguridad de la información, en el ámbito de los servicios de la Comunidad de Madrid y competencias de MD

Servicios y actividades a realizar:

- Soporte en la identificación de las normativas de seguridad de la información aplicables a los servicios de la Comunidad de Madrid, en el ámbito de competencias de MD.
 - Prestar apoyo a los responsables de MD en el desarrollo y mantenimiento de las aplicaciones que sustentan los servicios de la CM para:
 - Identificar la aplicabilidad de las posibles normativas de seguridad de la información.
 - Proponer los informes de aplicabilidad de las normativas de seguridad de la información, para su formalización por parte del responsable oportuno de la CM.
 - Interpretar los criterios de categorización de los sistemas ENS correspondientes de la CM, que incluya los referentes a la valoración de los activos esenciales (información y servicios) en cada una de las dimensiones que corresponda.
 - Generar los informes de categorización de los sistemas ENS, para su formalización por parte del responsable oportuno de la CM.
 - Caracterizar los activos que conforman los sistemas ENS.
- Generación de la declaración de aplicabilidad provisional.
 - Determinar las medidas de seguridad aplicables al sistema ENS, atendiendo a los resultados de la categorización realizada.
 - Prestar apoyo a los responsables de MD en el desarrollo y mantenimiento de las aplicaciones que sustentan los servicios de la CM en la interpretación y la implantación de las medidas de seguridad que se hayan determinado en cada caso.
- Supervisión de las actividades de adecuación y cumplimiento de las normativas de seguridad de la información.
 - Revisar la coherencia e idoneidad de todas las tareas anteriores que realizan los responsables de MD en el desarrollo y mantenimiento de las aplicaciones que sustentan los servicios de la CM, antes del paso a producción de las mismas.

4.1.4 Dominio: Análisis y gestión de riesgos de cumplimiento de seguridad de la información.

En este dominio se deberán realizar las siguientes de actividades generales, que permitirán abordar el resto de actividades de las capacidades de este dominio:

- Analizar la información disponible, y adquirir el conocimiento necesario, de la organización, de su estructura orgánica, de las competencias asignadas a cada unidad organizativa de MD y de los catálogos de servicios ofrecidos por MD, tanto a la CM como a la propia Agencia.
- Analizar la información disponible y adquirir el conocimiento necesario de la infraestructura TIC general de MD; infraestructuras físicas e infraestructura de Comunicaciones, de Sistemas, de arquitectura de aplicaciones y portales web, de los propios servicios TIC y del resto de servicios de soporte.

- Analizar la información disponible y adquirir el conocimiento necesario de todos los portales internos, herramientas corporativas o repositorios corporativos a través de los cuales se gestiona y almacena información de negocio y de inventario TIC.
- Analizar la información disponible y adquirir el conocimiento necesario de las aplicaciones y herramientas de MD empleadas en el ciclo de vida de los servicios TIC y de soporte (Ejemplos: herramientas para gestión de código fuente en el servicio de diseño y construcción de aplicaciones, herramientas de calidad del software y de pruebas de seguridad para el servicio de calidad y de paso a producción de las aplicaciones, herramientas de solicitud, gestión e instalación de certificados electrónicos para prestación de servicios electrónicos de confianza).

4.1.4.1 Capacidad: Análisis y gestión de riesgos de cumplimiento de seguridad de la información, en el ámbito de los sistemas ENS o servicios de MD

Servicios y actividades a realizar:

- Realización de los análisis de riesgos, conforme a MAGERIT y uso de la herramienta PILAR.
 - Verificar la caracterización realizada de los activos que conforman cada sistema ENS de MD.
 - Informar y valorar los activos e identificar las dependencias generadas entre ellos.
 - Obtener el riesgo potencial de los sistemas ENS a partir de las amenazas a las que están expuestos los activos que lo conforman.
 - Informar las medidas de seguridad o salvaguardas aplicables en cada caso, incluidas en la declaración de aplicabilidad correspondiente, y asignar la valoración de la madurez de cada medida implantada por el responsable del sistema.
 - Obtener el riesgo residual de los sistemas ENS.
 - Generar un informe de resultados del análisis de riesgos realizado.
 - Realizar el registro de los riesgos obtenidos, actualizando el registro de riesgos de cumplimiento de MD (RRI), y caracterizar cada uno de ellos para el tratamiento de los mismos y poder alcanzar el riesgo objetivo que se haya determinado.
- Análisis de los hallazgos recogidos en los informes de auditoría internos de cumplimiento de seguridad y en los informes de las distintas auditorías externas de seguridad realizadas.
 - Analizar la naturaleza de cada uno de los hallazgos identificados en las auditorías internas de cumplimiento de seguridad, actualizando el registro de riesgos de cumplimiento de MD (RRI), y caracterizar cada uno de ellos para el tratamiento de los mismos y poder alcanzar el riesgo objetivo que se haya determinado.
 - Analizar la naturaleza de cada uno de los hallazgos identificados en las auditorías externas, incluyendo las de certificación, actualizando el registro de riesgos de cumplimiento de MD (RRI), y caracterizar cada uno de ellos para el tratamiento de los mismos y poder alcanzar el riesgo objetivo que se haya determinado.

4.1.4.2 Capacidad: Identificación y gestión de riesgos de cumplimiento de seguridad de la información, en el ámbito de los servicios de la Comunidad de Madrid y competencias de MD

Servicios y actividades a realizar:

- Identificación de los principales riesgos existentes en el diseño y construcción de las aplicaciones de MD que soportan los servicios de la CM, mediante un proceso informal de análisis de los mismos.
 - Analizar y proponer los principales ámbitos de seguridad de la información sobre los que se plantea el análisis informal de los riesgos.
 - Analizar y proponer, por cada ámbito de seguridad definido, los principales escenarios de riesgos en los que plantear la exposición de posibles amenazas y la aplicación de las medidas de seguridad o salvaguardas que correspondan.
 - Supervisar la ejecución de cada análisis de riesgos realizado por los responsables de MD en el desarrollo y mantenimiento de las aplicaciones que sustentan los servicios de la CM y determinar y subsanar posibles incoherencias o falta de calidad de la información aportada a partir de los resultados obtenidos.
 - Generar un informe de resultados del análisis de riesgos realizado.
 - Realizar el registro de los riesgos obtenidos y caracterizar cada uno de ellos para el tratamiento de los mismos.

4.1.4.3 Capacidad: Gestión y seguimiento del registro de riesgos de cumplimiento de seguridad de la información, en el ámbito de servicios y de competencias de MD

Servicios y actividades a realizar:

- Valoración de los riesgos registrados en cada caso, a través de los distintos procesos establecidos (auditorías, análisis de riesgos MAGERIT-PILAR, análisis informal de riesgos, etc.) para proponer el estado de tratamiento que se le debe asignar en cada caso.
- Comprobación y valoración de la mitigación, parcial o total, o asunción de los riesgos, conforme a la información recibida acerca de la materialización de las distintas líneas de trabajo o actuaciones definidas para mitigar o reducir el riesgo.
- Propuesta de métricas e indicadores de seguimiento de la mitigación o asunción de los riesgos y elaboración del diseño de un cuadro de mando para realizar el seguimiento de esta cuestión.

4.1.5 Dominio: Planes y programas de seguridad de la información.

4.1.5.1 Capacidad: Elaboración y despliegue de los Planes y Programas de Seguridad de MD

Servicios y actividades a realizar:

- Análisis de los registros de riesgos dados de alta o de los ya existentes en el RRI, procedentes de los distintos análisis de riesgos realizados o de los distintos hallazgos que se hayan identificado en las auditorías, internas o externas, de cumplimiento de seguridad.

- Analizar la naturaleza de cada uno de los registros de riesgos que se hayan incluido en el RRI y asignar la información necesaria para determinar las actuaciones que se consideren necesarias para mitigar el riesgo.
- Incorporar todas las actuaciones definidas en la mitigación de los riesgos en los planes y programas de seguridad de MD.
- Análisis de los hallazgos recogidos en los informes de auditoría de certificación externa y elaboración de los Planes de Acciones Correctoras (PAC) requeridos.
 - Analizar la naturaleza de cada uno de los hallazgos identificados en las auditorías de certificación externa, tanto de la norma UNE-EN ISO/IEC 27001:2023 como del ENS, determinar las acciones mitigadoras asociadas a cada una de ellas y proponer toda la información asociada a las mismas que se recogen en las fichas de Planes de Acciones Correctoras (PAC) para remitirlos a la entidad auditora de certificación.
- Despliegue de los Planes y Programas de Seguridad de MD.
 - Elaborar la documentación necesaria con el detalle de toda la información asociada a las actuaciones necesarias para realizar la mitigación de los riesgos identificados en el RRI, incluyendo la determinación de los indicadores de seguimiento de ejecución de las actuaciones.
 - Planificar las reuniones, de inicio y de seguimiento, con las Unidades Organizativas de MD que deben responsabilizarse o intervenir en la ejecución de las actuaciones definidas.
 - Participar y preparar la documentación necesaria para mantener las reuniones de inicio o de seguimiento de ejecución de las actuaciones definidas.

4.1.5.2 Capacidad: Seguimiento de ejecución de los Planes y Programas de Seguridad de MD

Servicios y actividades a realizar:

- Análisis, recopilación e información de los indicadores de seguimiento de ejecución de las actuaciones definidas dentro de los planes y programas de seguridad.
 - Analizar el estado de situación de la ejecución de las actuaciones definidas e informar, en cada caso, los valores de los indicadores definidos para realizar el seguimiento de ejecución.
 - Propuesta de métricas para realizar un seguimiento global de los planes y programas de seguridad, permitiendo tener una visión completa, gradual y pormenorizada de los distintos componentes definidos dentro de los planes y programas.
 - Proponer y elaborar el diseño de un cuadro de mando para realizar el seguimiento global de los planes y programas de seguridad.

4.2 Ámbito de PREVENCIÓN:

4.2.1 Dominio: Normativa de seguridad de la información.

4.2.1.1 Capacidad: Desarrollo y gestión del cuerpo normativo de seguridad de la información de MD

Servicios y actividades a realizar:

- Identificación de nuevas necesidades de documentación, inventario y gestión del cambio del cuerpo normativo:
 - Actualizar y mantener el mapa del cuerpo normativo de seguridad de la información de MD.
 - Actualizar y mantener el inventario del cuerpo normativo, con toda su información de detalle de cada uno de sus documentos.
 - Revisar los registros de documentación existentes en el inventario a fin de identificar desactualizaciones y carencias de los documentos.
 - Proponer y registrar las actuaciones necesarias para solventar aquellas cuestiones que se hayan determinado en el análisis de los registros de la documentación.
- Elaboración de nueva documentación del cuerpo de seguridad de la información de MD.
 - Analizar en profundidad la nueva necesidad regulatoria de seguridad, determinar el contenido objeto de normalización y elaborar los documentos normativos cuya responsabilidad recaen sobre el área de GRC de seguridad. Fundamentalmente, se tratará de documentación de aplicación general y que se formalizará a través de documentos de alcance general dentro de la estructura normativa de la documentación corporativa de MD (Documentos Marco y Documentos de competencia).
 - Analizar en profundidad la nueva necesidad regulatoria de carácter operativo de seguridad. En el caso de que la responsabilidad operativa recaiga en la propia Subdirección General de Ciberseguridad se deberá determinar el contenido objeto de esta necesidad y elaborar los documentos operativos correspondientes. En el caso de que la responsabilidad operativa recaiga en cualquier otra Unidad Organizativa de MD se prestará a su responsable el soporte necesario y la coordinación necesario con otras Unidades intervinientes para apoyarle y ayudarle en la generación de la documentación final.

En ambos casos, fundamentalmente, se formalizará a través de documentos de carácter operativo dentro de la estructura normativa de la documentación corporativa de MD (Procedimientos y Documentos de especificaciones).

4.2.2 Dominio: Formación y concienciación en materia de seguridad de la información.

4.2.2.1 Capacidad: Identificación de necesidades en materia de seguridad de la información para los planes de formación de MD.

Servicios y actividades a realizar:

- Identificación de necesidades en materia de formación para MD y, en particular, para la SGCPDP.

- Dar soporte en la identificación de necesidades de formación en materia de seguridad de la información para el personal de MD.
- Dar soporte en la elaboración de información y en la documentación de las distintas propuestas de cursos y temarios de seguridad de la información.

4.2.2.2 Capacidad: Sensibilización y Concienciación de Seguridad de la información

Servicios y actividades a realizar:

- Análisis de necesidades de concienciación y sensibilización de seguridad de la información de MD.
 - Proponer acciones de concienciación y sensibilización de seguridad para el personal de MD y de la CM atendiendo a:
 - o Las principales amenazas existentes asociadas a ataques basados en ingeniería social.
 - o La normativa y buenas prácticas en materia de seguridad de la información.
 - o Novedades en la regulación de seguridad, propia o externa, o relacionadas con cuestiones de la propia Agencia relativas a la seguridad de la información.
- Diseño y elaboración del Plan anual de sensibilización y concienciación de seguridad de la información de MD.
 - Impulsar, promover y mejorar la cultura de seguridad de la información en Madrid Digital.
 - Proponer un plan de sensibilización y concienciación de seguridad de la información con la planificación y el detalle del contenido de cada acción de concienciación prevista (campañas de difusión de concienciación, publicación en portales y espacios colaborativos de contenido de seguridad, ejercicios y simulaciones de seguridad, etc.)
 - Elaborar la documentación de las distintas acciones de concienciación de seguridad de la información programadas.
 - Analizar la necesidad de emplear herramientas especializadas en realizar campañas de concienciación y seleccionar las más adecuadas en cada caso.
- Diseño, elaboración y ejecución de campañas de difusión, sensibilización y concienciación de seguridad de la información.
 - Elaborar la documentación de las distintas campañas, píldoras, ejercicios, simulaciones o mensajes de concienciación de seguridad de la información para el personal de MD y de la CM.
 - Configurar los parámetros necesarios de las herramientas seleccionadas para realizar las campañas de concienciación en Madrid Digital.
 - Ejecutar las distintas campañas de concienciación realizando un seguimiento de las mismas y analizando el resultado de las mismas para reportar a la SGCPDP.
 - Realizar sesiones de formación y/o concienciación al personal de la Agencia en relación con las necesidades identificadas en materia de seguridad de la información y con las campañas realizadas.

4.2.3 Dominio: Asesoría en seguridad de la información.

4.2.3.1 Capacidad: Asesoramiento, legal y técnico, en los distintos ámbitos de seguridad de la información.

Servicios y actividades a realizar:

- Valoración y respuesta de las consultas o peticiones recibidas en materia de seguridad de la información:
 - Analizar y valorar las consultas o peticiones recibidas, en materia de seguridad de la información, desde cualquier ámbito de actividad de las Subdirecciones Generales o de las Direcciones de MD.
 - Proponer la planificación de tiempo para realizar la documentación de respuesta a cada petición o consulta recibida.
 - Elaborar cuanta documentación sea necesaria para dar respuesta según el criterio adoptado por el área de GRC de Seguridad de la información.
 - Actualizar y mantener el inventario de todas las consultas o peticiones recibidas, con toda su información de detalle de cada una de ellas (peticionario, fecha de solicitud, planificación propuesta de respuesta y tipo de documentación generada, documentación final de respuesta, etc).
- Valoración y soporte a las consultas o peticiones recibidas por la Consejería Delegada y/o por la Dirección de Servicios Jurídicos de MD:
 - Analizar y valorar las consultas o peticiones de seguridad de la información provenientes de la Consejería Delegada de MD y/o de la Dirección de Servicios Jurídicos de MD. Las consultas o peticiones podrán estar relacionadas con solicitudes de los Cuerpos y Fuerzas de Seguridad del Estado, con requerimientos judiciales o con solicitudes de los titulares de los Centros Directivos de la CM.
 - Proponer la planificación de tiempo para realizar la documentación de respuesta a cada petición o consulta recibida.
 - Elaborar cuanta documentación sea necesaria para dar respuesta según el criterio adoptado por el área de GRC de Seguridad de la información.
 - Actualizar y mantener el inventario de todas las consultas o peticiones recibidas, con toda su información de detalle de cada una de ellas (peticionario, fecha de solicitud, planificación propuesta de respuesta y tipo de documentación generada, documentación final de respuesta, etc).

4.2.4 Dominio: Excepciones de cumplimiento de seguridad de la información.

4.2.4.1 Capacidad: Análisis y Soporte a las solicitudes de excepción de cumplimiento de la normativa de seguridad de la información.

Servicios y actividades a realizar:

- Análisis de las consultas acerca de las solicitudes de ***excepción de cumplimiento de la normativa de seguridad de la información***:

- Estudiar la naturaleza y el impacto de las posibles solicitudes recibidas por la Subdirectora de Ciberseguridad en lo referente a propuestas de excepción de cumplimiento de la normativa de seguridad de la información.
- Elaborar cuanta documentación sea necesaria para proponer asumir, o no, los riesgos derivados de dichas excepciones.
- Elaborar la documentación necesaria para realizar propuestas al Comité de Dirección para asumir aquellos riesgos que, por distintas circunstancias, su tratamiento y mitigación no ha sido posible concluir y es necesario plantear la aceptación del riesgo por la Dirección para su formalización.

4.3 Ámbito de DETECCIÓN:

4.3.1 Dominio: Auditorías de cumplimiento de seguridad de la información.

4.3.1.1 Capacidad: Apoyo y soporte en la definición y actualización del plan anual de auditoría y ejecución del plan interno de auditoría.

Servicios y actividades a realizar:

- Apoyo en la definición del plan anual de auditoría de cumplimiento de seguridad en MD.
 - Elaborar cuanta documentación sea necesaria para realizar la propuesta del Plan anual de auditoría de MD a la SGCPDP.
- Apoyo técnico en la ejecución del plan interno de auditoría de cumplimiento de seguridad en MD.
 - Apoyar al equipo de auditoría de MD en el análisis y descubrimiento de los activos y recursos TIC de MD que serán objeto de auditoría y colaborar en esta actividad con el equipo de auditoría del adjudicatario del LOTE 2 “Servicios de auditoría y verificación de cumplimiento de seguridad de la información”.
 - Analizar cuantas cuestiones, dudas o problemas surjan de la planificación y ejecución del plan interno de auditoría respecto de las posibles consultas o peticiones que le pudiera surgir al equipo externo de auditor (ver LOTE 2 “Servicios de auditoría y verificación de cumplimiento de seguridad de la información”).
 - Elaborar cuanta documentación sea necesaria para impulsar la ejecución de los trabajos previstos en el LOTE 2 Servicios de auditoría y verificación de cumplimiento de seguridad de la información.
 - Acompañar al equipo de auditoría de MD en todas las actividades y reuniones que resulten de la ejecución del plan interno de auditoría.
 - Realizar la supervisión de la ejecución del plan interno de auditoría reportando de forma continua al responsable del servicio de auditoría de MD.
 - Apoyar al equipo de auditoría de MD en la revisión de la documentación generada durante la ejecución de los trabajos previstos en el LOTE 2 “Servicios de auditoría y verificación de cumplimiento de seguridad de la información”.
 - Elaborar cuanta documentación sea necesaria para realizar el seguimiento y supervisión de la ejecución del plan interno de auditoría.

Todos los servicios y actividades a realizar que se han descrito son objeto de prestación por parte del equipo base de este lote.

4.4 SERVICIOS DE CUOTA FIJA Y VARIABLE.

Los trabajos requeridos en este LOTE se ejecutarán a través de servicios de cuota fija y servicios de cuota variable según lo siguiente:

- **Servicios de cuota fija:** incluye la realización de todos los trabajos que sean necesarios, a través del denominado Equipo Base (ver cláusula 7, Equipo de Trabajo), para ejecutar todos los servicios y actividades previstas en cada una de las capacidades descritas anteriormente.
- **Servicios de cuota variable:** incluye la realización de todos los trabajos que sean necesarios, a través del denominado Equipo de Proyecto (ver cláusula 7, Equipo de Trabajo), para atender a las líneas de actuación o proyectos no planificados que requiera MD y el apoyo, refuerzo o especialización que pudiera requerir de los trabajos del servicio de cuota fija.

CLÁUSULA 5. LOTE 2: SERVICIOS DE AUDITORÍA Y VERIFICACIÓN DE CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN.

La actividad de los servicios de auditoría y verificación de cumplimiento de seguridad de la información se centrará en la adquisición, mejora y desarrollo de determinadas capacidades del modelo de ciberseguridad de MD correspondientes al ámbito de detección, y de sus líneas de servicio asociadas, que tienen por objeto el ejercicio de las competencias de la SGCPDP en materia de GRCSI.

El equipo de auditoría de MD determinará la periodicidad con la que se realizarán las auditorías de cumplimiento de las distintas normas de seguridad que se detallan más adelante.

Los trabajos a realizar se estructurarán en las siguientes **fases**:

CUOTA FIJA:

- Elaboración de programas de auditoría de cumplimiento y planificación del servicio. **A realizar durante 3 meses.**
- Ejecución de las auditorías, presentación de resultados y hallazgos de auditoría y atención a las alegaciones de los interesados. **A realizar durante 12 meses a contar desde la finalización de la fase anterior.**

CUOTA VARIABLE:

- Implantación de las acciones correctoras por parte de los equipos de MD y subsanación de los hallazgos. Soporte de los auditores a los interesados en la remediación de los hallazgos. **A realizar, durante 6 meses, desde la finalización de la fase anterior.**
- Verificación de implantación de las acciones correctoras y subsanación de los hallazgos y ejecución de auditorías extraordinarias. **A realizar los últimos 12 meses del contrato.**

En caso de **prórroga** del contrato los servicios a realizar serán únicamente los correspondientes a la cuota variable.

El adjudicatario de este lote llevará a cabo, bajo la dirección de MD, los siguientes servicios y actividades:

5.1 Ámbito de DETECCIÓN:

5.1.1 Dominio: Auditorías de cumplimiento de seguridad de la información.

5.1.1.1 Capacidad: Planificación y elaboración del Plan interno de auditoría.

Servicios y actividades a realizar:

- Planificación detallada de la ejecución de las auditorías de cumplimiento de seguridad de la información.
 - Realizar una propuesta completa de las auditorías de cumplimiento de las normativas de seguridad con un enfoque orientado a controles o medidas de seguridad. Con carácter de mínimos, se deberá incluir el Esquema Nacional de Seguridad (RD 311/2022), la UNE-EN ISO/IEC 27001:2023, los criterios generales de seguridad que han de contemplar según acuerdo del Pleno, de 13 de septiembre de 2007, del Consejo General del Poder Judicial para los SS.II. al servicio de la Administración de Justicia.
 - Concretar la clasificación de los controles o medidas según el carácter de cada una de las normativas. Se deberá identificar y justificar de forma detallada si la aplicación de cada control o medida es transversal a todos los activos afectados por las auditorías, si es específico de cada uno de ellos o si es de carácter mixto (de aplicación transversal y específico).
 - Establecer la planificación de las auditorías según la propuesta realizada, referida en el primer punto, dando prioridad a la revisión de los controles o medidas de carácter transversal.
 - Analizar el catálogo de los distintos servicios de MD que serán objeto de auditoría. MD facilitará, al inicio del proyecto, dicho catálogo de servicios. A lo largo del contrato, dicho catálogo podrá ampliarse a aquellos nuevos servicios que se formalicen en MD o a aquellos otros que puedan identificarse con posterioridad y que, por cualquier motivo, no hubieran sido incluidos en el mencionado catálogo.
 - Analizar el catálogo de los SS.II. que serán objeto de auditoría por encontrarse en el alcance de aplicación de las normativas de seguridad que se hayan determinado en la propuesta inicial realizada. MD facilitará, al inicio del proyecto, dicho catálogo de SS.II. A lo largo del contrato, dicho catálogo podrá ampliarse a aquellos nuevos SS.II. que se incorporen en el alcance de las normativas auditadas o a aquellos otros que puedan identificarse con posterioridad y que, por cualquier motivo, no hubieran sido incluidos en el mencionado catálogo.
 - Identificar las distintas agrupaciones de activos que pueden ser objeto de auditoría por soportar o formar parte de los servicios de MD que son objeto de la auditoría (activos tecnológicos transversales, activos de SS.II. propios, activos de SS.II de terceros, activos de servicios TIC,).
 - Identificar toda la información asociada a cada activo a auditar que pueda residir en los inventarios técnicos de MD o en las propias áreas internas de MD. En base a esta información se deberá completar la estimación y planificación de cada auditoría.

- Proponer la planificación global de la ejecución anual de las auditorías de cumplimiento, así como la priorización de ejecución, atendiendo a la complejidad y envergadura de los activos a auditar.
- Elaborar y actualizar, de forma permanente, el plan interno de auditoría de MD, que debe incluir información concreta sobre la gestión, registro y seguimiento de la ejecución de las auditorías.
- Elaborar cuanta documentación sea necesaria para realizar la presentación o el reporte de los trabajos planificados.

5.1.1.2 Capacidad: Ejecución de las auditorías de cumplimiento de seguridad de la información.

Servicios y actividades a realizar:

- Conocimiento de la organización y del entorno TIC.
 - Analizar la información disponible, y adquirir el conocimiento necesario, de la organización, de su estructura orgánica, de las competencias asignadas a cada unidad organizativa de MD y de los catálogos de servicios ofrecidos por MD, tanto a la CM como a la propia Agencia.
 - Analizar la información disponible y adquirir el conocimiento necesario de la infraestructura TIC general de MD; infraestructuras físicas e infraestructura de Comunicaciones, de Sistemas, de arquitectura de aplicaciones y portales web, de los propios servicios TIC y del resto de servicios de soporte.
 - Analizar la información disponible y adquirir el conocimiento necesario de todos los portales internos, herramientas corporativas o repositorios corporativos a través de los cuales se gestiona y almacena información de negocio y de inventario TIC.
 - Analizar la información disponible y adquirir el conocimiento necesario de las aplicaciones y herramientas de MD empleadas en el ciclo de vida de los servicios TIC y de soporte (Ejemplos: herramientas para gestión de código fuente en el servicio de diseño y construcción de aplicaciones, herramientas de calidad del sw y de pruebas de seguridad para el servicio de calidad y de paso a producción de las aplicaciones, herramientas de solicitud, gestión e instalación de certificados electrónicos para prestación de servicios electrónicos de confianza).
 - Analizar la información disponible y adquirir el conocimiento necesario de todos riesgos de cumplimiento de seguridad registrados hasta la fecha en el Registro de Riesgos Identificados de MD (RRI-MD).
 - Analizar la información disponible y adquirir el conocimiento necesario de todas las Declaraciones de Aplicabilidad asociadas a los distintos sistemas de MD (servicio + información) a auditar.
 - Analizar la información disponible y adquirir el conocimiento necesario de todas las evidencias de auditoría de cumplimiento de seguridad registradas hasta la fecha en el repositorio unificado de evidencias de auditoría de MD.
 - Proponer un planteamiento integral de auditoría de cumplimiento de seguridad en MD, que incluya la identificación de toda la normativa a auditar, los controles o medidas a

- auditar según su clasificación y aplicabilidad y la posible propuesta de perfiles de cumplimiento de los activos afectados.
- Elaborar cuanta documentación sea necesaria para realizar la presentación o el reporte de los trabajos realizados.
 - Concreción de la planificación de las auditorías de cumplimiento de seguridad de la información.
 - Proponer la planificación particular de la ejecución de cada auditoría de cumplimiento atendiendo a toda la información y el conocimiento adquirido incluyendo toda la información de detalle necesaria para lanzar las convocatorias de inicio de los trabajos de auditoría.
 - Elaborar el programa detallado de cada auditoría con la descripción de las pruebas y verificaciones a realizar para verificar la existencia e implantación de los controles o medidas de seguridad correspondientes.
 - En particular, se deberá realizar una propuesta de pruebas concretas sobre las herramientas, consolas, repositorios o cualquier otro componente que evidencie de forma contundente el cumplimiento de aquellos controles donde proceda realizar estas comprobaciones. Asimismo, se deberá proponer las pruebas destinadas a la verificación de cumplimiento de la aplicación de la normativa y de los procedimientos e instrucciones técnicas vigentes, formalizadas o no, que determinan la forma de gobierno, de gestión y de operación de todos los servicios TIC y de sus activos.
 - Preparar todas las convocatorias de reunión necesarias para ejecutar las auditorías previstas, que incluya toda la información y documentación necesaria para mantener las reuniones posteriores.
 - Concretar el formato y contenido de los informes de resultados de auditoría, debiendo cumplir los requisitos y criterios del equipo de auditoría de MD de cara a poder extraer posteriormente información para realizar el reporte requerido por Organismos internos de la CM y por Organismos externos reguladores.
 - Mantener reuniones preliminares con los responsables de los activos auditados, con antelación a las reuniones de auditoría, con el fin de confirmar o verificar el alcance de la auditoría y las responsabilidades en los distintos ámbitos de los activos (gobierno, gestión, operación, etc).
 - Generar cuantas actas sean necesarias para dejar documentado lo tratado en todas las reuniones mantenidas.
 - Ejecución de la planificación de las auditorías de cumplimiento de seguridad de la información.
 - Enviar las convocatorias de reunión preparadas y mantener reuniones de auditoría con los responsables de los activos auditados y realizar todas las pruebas definidas y previstas en el programa detallado de auditoría.
 - Generar cuantas actas sean necesarias para dejar documentado lo tratado en todas las reuniones mantenidas.

- Enviar a los auditados, con posterioridad a las reuniones de auditoría mantenidas, el acta correspondiente y el requerimiento de las evidencias que se hayan identificado como necesarias en el transcurso de las reuniones de auditoría.
- Realizar un seguimiento de las evidencias solicitadas, mantener el registro de todo ello de forma que se pueda consultar de forma ágil y sencilla y requerir de nuevo esta información en caso de no recibirla.
- Registrar, siguiendo las indicaciones y el criterio del equipo de auditoría de MD, las evidencias obtenidas en las distintas auditorías realizadas.
- Elaborar, y enviar a los afectados, los informes de resultados de auditoría conforme al formato y contenido previamente acordado.
- Informar a los afectados de los plazos para poder remitir consultas, dudas o reclamaciones de los informes de resultados de auditoría.
- Atender las consultas, dudas o reclamaciones de los responsables auditados respecto de los resultados de auditoría que les hayan sido comunicados.
- Realizar un seguimiento de los envíos realizados con los informes de resultados de auditoría, de los responsables en cada caso, de los plazos asignados para remitir consultas, dudas o reclamaciones y mantener el registro de todo ello de forma que se pueda consultar de forma ágil y sencilla.
- Elaborar cuanta documentación sea necesaria para realizar la presentación o el reporte de los trabajos realizados y de los resultados obtenidos.

5.1.2 Dominio: Revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información.

5.1.2.1 Capacidad: Planificación y ejecución de las revisiones, verificaciones o diagnósticos de seguridad.

Servicios y actividades a realizar:

- Identificación de necesidades y planificación de la ejecución de las revisiones, verificaciones o diagnósticos de seguridad. La naturaleza de estos trabajos podrá estar relacionada con cualquier materia relacionada con la seguridad de la información:
 - Realizar el análisis y estimación de los requerimientos de MD para ejecutar revisiones, verificaciones o diagnósticos de seguridad que, en cada caso, MD estime necesarias.
 - Preparar y entregar una propuesta de trabajo con la información de las fases de trabajo, el detalle de actividades a realizar, la estimación de perfiles y número de personas del equipo de trabajo, el número de horas estimado en cada caso y la planificación propuesta.
 - Recabar el visto bueno de MD de las propuestas de trabajo para poder estar en disposición de iniciar los trabajos.
 - Elaborar cuanta documentación sea necesaria para realizar la presentación o el reporte de los trabajos planificados.

- Ejecución de las revisiones, verificaciones o diagnósticos de seguridad.
 - Mantener reuniones de inicio de los trabajos con los responsables de los servicios o de los activos afectados por la revisión, verificación o diagnóstico de seguridad para informar del alcance los trabajos y confirmar las responsabilidades afectadas por las distintas unidades organizativas de MD.
 - Preparar y enviar las convocatorias de reunión preparadas y mantener reuniones de trabajo con los responsables afectados y realizar todas las actividades previstas en la propuesta de trabajo correspondiente.
 - Generar cuantas actas sean necesarias para dejar documentado lo tratado en todas las reuniones mantenidas.
 - Enviar a los responsables afectados por el alcance de los trabajos, con posterioridad a las reuniones mantenidas, el acta correspondiente y el requerimiento de la información y de las evidencias que se hayan identificado como necesarias.
 - Realizar un seguimiento de las evidencias solicitadas, mantener el registro de todo ello de forma que se pueda consultar de forma ágil y sencilla y requerir de nuevo esta información en caso de no recibirla.
 - Registrar, siguiendo las indicaciones y el criterio del equipo de auditoría de MD, las evidencias obtenidas en las distintas revisiones, verificaciones o diagnósticos de seguridad.
 - Elaborar, y enviar a los afectados, los informes de resultados de los trabajos realizados conforme al formato y contenido previamente acordado con MD.
 - Informar a los afectados de los plazos para poder remitir consultas, dudas o reclamaciones de los informes de resultados recibidos.
 - Atender las consultas, dudas o reclamaciones de los responsables auditados respecto de los informes de resultados.
 - Realizar un seguimiento de los envíos realizados con los informes de resultados, de los responsables en cada caso, de los plazos asignados para remitir consultas, dudas o reclamaciones y mantener el registro de todo ello de forma que se pueda consultar de forma ágil y sencilla.
 - Elaborar cuanta documentación sea necesaria para realizar la presentación o el reporte de los trabajos realizados y de los resultados obtenidos.

CLÁUSULA 6. LOTE 3: SERVICIOS DE AUDITORÍA DE CERTIFICACIÓN DE CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN. (CUOTA VARIABLE)

La actividad de los servicios de auditoría de certificación de cumplimiento de las normas de seguridad de la información se centrará en la adquisición, mejora y desarrollo de determinadas capacidades del modelo de ciberseguridad de MD correspondientes al ámbito de detección, y de sus líneas de servicio asociadas, que tienen por objeto el ejercicio de las competencias de la SGCPDP en materia de GRCSI. El fin último de los servicios es obtener la certificación que acredite el cumplimiento de las normas de seguridad de la información que MD determine respecto de los propios servicios de MD, prestados tanto a la CM como internamente.

El adjudicatario de este lote llevará a cabo, bajo la dirección de MD, las siguientes actividades:

6.1 Ámbito de PREVENCIÓN:

6.1.1 Dominio: Formación y concienciación en materia de seguridad de la información.

6.1.1.1 Capacidad: Identificación de necesidades en materia de seguridad de la información para los planes de formación de MD.

Servicios y actividades a realizar:

- Identificación de necesidades en materia de formación para MD y, en particular, para la SGCPDP.
 - Proponer necesidades y ciclos de formación en materia de seguridad de la información para el personal de MD. Especialmente en normativas y buenas prácticas de aplicación como son ENS, UNE-ISO 27001, NIST2, Análisis de Riesgos de cumplimiento de seguridad de la información.
 - Facilitar la información y la documentación de las distintas propuestas de cursos y temarios de seguridad de la información.
- Ejecución de acciones y cursos de seguridad de la información, en particular, para la SGCPDP.

6.2 Ámbito de DETECCIÓN:

6.2.1 Dominio: Auditoría de certificación de cumplimiento de normas de seguridad de la información.

6.2.1.1 Capacidad: Planificación y ejecución de análisis GAP y de las auditorías de certificación.

Servicios y actividades a realizar:

- Identificación de necesidades y planificación de la ejecución de los análisis GAP y de las auditorías de certificación de cumplimiento de normas de seguridad de la información. La naturaleza de estos trabajos podrá estar relacionada con cualquier norma certificable relacionada con la seguridad de la información:
 - Realizar la valoración y estimación de los requerimientos de MD para realizar los análisis GAP y las auditorías de certificación de cumplimiento de normas de seguridad de la información.
 - Preparar y entregar una propuesta de trabajo con toda la información necesaria para llevar a cabo el Plan de Trabajo definido por la entidad acreditadora.
 - Recabar el visto bueno de MD de las propuestas de trabajo para poder estar en disposición de iniciar los trabajos.
- Ejecución de los análisis GAP y de las auditorías de certificación de cumplimiento de normas de seguridad de la información:
 - Requerir a MD la información y documentación necesaria para realizar las fases de auditoría documental que, en cada caso, se precise.
 - Mantener reuniones de trabajo de campo de auditoría con los responsables afectados de MD y realizar todas las actividades previstas en el plan de trabajo correspondiente.

- Elaborar, y enviar al área de GRCSI, los distintos informes de resultados que se generen.
- Informar al área de GRCSI de los plazos para que ésta pueda remitir consultas, dudas o reclamaciones de los informes de resultados recibidos, así como requerir al área de GRCSI el envío de los Planes de Acciones Correctoras (PAC) necesarios en caso de identificarse no conformidades.
- Confirmar al área de GRCSI el cierre de los trabajos con la finalización de todos sus aspectos relacionados.
- Comunicar al área de GRCSI el dictamen o resultado final de cada análisis GAP y de la auditoría de certificación realizada.

CLÁUSULA 7. EQUIPO DE TRABAJO

Para desempeñar los servicios objeto de cada uno de los lotes del pliego, cada uno de los adjudicatarios contará con una capacidad productiva de forma que garanticen el nivel de especialización requerido para la prestación del servicio, y por la capacidad productiva back-office que sea necesaria aportar por parte del adjudicatario, más allá de los integrantes de los propios equipos, 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.

7.1 LOTE 1: Servicios de la Oficina de Gobierno de Seguridad (OGS)

El adjudicatario pondrá a disposición de Madrid Digital **dos tipos de equipos de personas: Base (Cuota fija) y Proyecto (Cuota variable).**

CUOTA FIJA:

- **Gestión del Servicio Continuo** del equipo de trabajo denominado **Equipo Base de proyecto** de la OGS. El adjudicatario constituirá el Equipo Base con las capacidades y perfiles necesarios definidos y se encargará de:
 - Prestación del servicio continuo de dirección, coordinación y seguimiento para el gobierno del servicio de la OGS.
 - Prestación del servicio continuo de dirección y coordinación del servicio de la OGS en el ámbito de los servicios de auditoría y gestión de riesgos de seguridad.
 - Prestación del servicio continuo de dirección y coordinación del servicio de la OGS en el ámbito de los servicios de normativa, planes y programas de seguridad.
 - Prestación del servicio continuo en la adquisición, mejora y desarrollo de las capacidades de seguridad de los ámbitos de gobierno, prevención y detección en materia GRCSI definidas en la cláusula 4.

La constitución del **Equipo Base** deberá realizarse desde el mismo momento de la firma del contrato.

El adjudicatario estará obligado a poner a disposición de Madrid Digital los recursos que integren este equipo desde ese mismo momento. El incumplimiento de esta obligación, tanto en número de personas como en la cualificación profesional de las mismas, dará lugar a la penalización correspondiente.

CUOTA VARIABLE:

- **Gestión de Proyectos o Servicios no planificados** del equipo de trabajo denominado **Equipo Proyecto**, para atender a las líneas de actuación o proyectos no planificados (cuota variable) que requiera MD.

El número de máximo de horas estimado por categorías para los servicios no planificados (cuota variable), por anualidades es el siguiente:

Gestión de Proyectos (Cuota VARIABLE) - Equipo PROYECTO Dedicaciones necesarias Proyectos					
Perfiles Profesionales	HORAS 2025 (4 meses)	HORAS 2026 (12 meses)	HORAS 2027 (12 meses)	HORAS 2028 (8 meses)	HORAS TOTALES (36 meses)
Consultor Senior	800	3.200	3.200	2.400	9.600
Ingeniero de Seguridad	933	3.733	3.733	2.801	11.200
HORAS TOTALES	1.733	6.933	6.933	5.201	20.800

Cuando el responsable de Gobierno del Servicio de MD requiera, formalmente y por escrito, al responsable del Servicio del adjudicatario abordar un proyecto variable, **antes de 8 días laborables**, este último tendrá que **enviar a MD una carta de encargo con la propuesta de las condiciones y estimaciones correspondientes**. Deberá realizarse una descripción detallada de los objetivos del proyecto, de las actividades y tareas a realizar, de los entregables comprometidos, así como la cuantificación del esfuerzo, medido en horas/recurso por cada uno de los perfiles profesionales propuestos. Corresponderá al responsable de Gobierno del Servicio de MD valorar su contenido quedando bajo su discreción incorporar las modificaciones que considere oportunas. En caso de discrepancia, prevalecerá el criterio razonado y documentado del responsable de Gobierno del Servicio de MD, salvo que la desviación sea igual o superior a dos terceras partes de lo estimado por el responsable del Servicio del adjudicatario, caso en el que se elevará al Comité de Seguimiento del Contrato el cual decidirá el criterio en base a los informes razonados de ambas partes.

El retraso en la entrega de la carta de encargo de un proyecto variable más allá del tiempo antes mencionado, 8 días laborables, dará lugar a la penalización correspondiente.

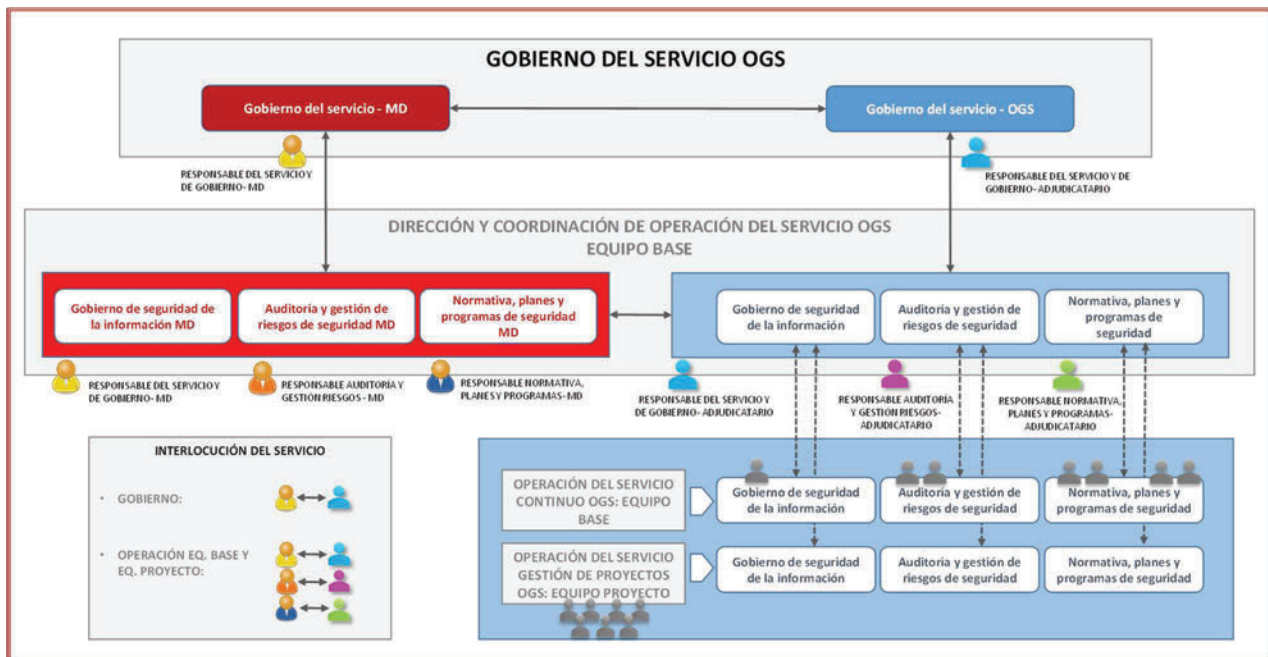
La formalización de cada proyecto variable se realizará a través de la aprobación del responsable de Gobierno del Servicio de MD.

Cuando el responsable de Gobierno del Servicio de MD comunique al responsable del Servicio del adjudicatario la aprobación y necesidad de inicio de un proyecto conforme a la carta de encargo, **antes de 12 días laborables, deberá haberse constituido el equipo de trabajo.**

Los equipos de Proyecto podrán constituirse en número variable de componentes sobre la base de cualquier combinación de perfiles profesionales contemplados en el pliego.

El adjudicatario estará obligado a poner a disposición de Madrid Digital 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.

A continuación, se resume la organización de gobierno y de operación del servicio continuo y de gestión de proyectos de la OGS:



El responsable de MD, en cada uno de los ámbitos de servicio indicados anteriormente, establecerá e informará al adjudicatario la necesidad de que el personal de los equipos se desplace el tiempo que considere necesario para mantener reuniones de trabajo o de seguimiento, realizar presentaciones o cualquier otra cuestión que considere oportuna para el buen desarrollo del servicio y a lo largo de todo el contrato.

Queda bajo el criterio exclusivo de MD realizar los cambios que considere en base a los efectivos disponibles y a los plazos comprometidos por Madrid Digital en cada caso.

El adjudicatario asumirá que todos los proyectos y servicios a desarrollar por el adjudicatario 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 Madrid Digital.

Equipo Base (de Cuota Fija): Líneas de actuación y actividades a desarrollar.

El equipo base se conformará de diez (10) recursos, que deberán cumplir con carácter de mínimos el perfil profesional requerido para cada línea de actividad de la OGS:

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Responsable del servicio y de la OGS	Jefe de Proyecto (Servicio y gobierno)	1 recurso al 33% de la duración del proyecto. La dedicación de este perfil implica prestar soporte en todos los servicios del ámbito de gobierno y asumir las tareas propias del gobierno del propio servicio integral del proyecto prestado por el adjudicatario.
EXPERIENCIA		
Al menos ocho (8) 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá disponer de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> • Título homologado por el CNP de Director de Seguridad. <p>Asimismo, deberá contar con, al menos, dos de las siguientes referencias:</p> <ul style="list-style-type: none"> • CISM (Certified Information Security Manager) de ISACA. • CISA (Certified Information Security Auditor) de ISACA. • Certificación Auditor Líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). En todos los casos deberá estar certificado en la versión vigente de la norma UNE-ISO 27001. • Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> • Liderazgo y coordinación de equipos multidisciplinares de trabajo, planificación, seguimiento y control de actividades en proyectos de oficina de gobierno de seguridad con afectación en el ámbito de marcos normativos de ciberseguridad, seguridad de la información, protección de datos, protección de infraestructuras estratégicas, críticas y servicios esenciales (funciones GRC de Gobierno, Riesgo y Cumplimiento). • Conocimientos de la normativa y buenas prácticas de seguridad de la información, especialmente del ENS, UNE-EN ISO/IEC 27001:2023 y normativa LPIC, a través de los respectivos cursos de formación realizados (al menos, 80 horas en cada uno de los tres ámbitos). • Conocimiento de herramientas de cuadros de mando. • Experiencia en definición de cuadros de mando de seguridad, avalada por, al menos 3 proyectos en clientes. • Conocimiento de herramientas de mercado GRC de seguridad de la información. • Conocimiento de las herramientas de seguridad del CCN, CNPIC y AEPD. • Experiencia en la elaboración de planes directores de seguridad y en la elaboración de normativas y procedimientos de seguridad de la información, avalada por, al menos 3 proyectos en clientes. • Experiencia en proyectos de adecuación a la UNE-EN ISO/IEC 27001:2023 y al ENS, avalada por, al menos 3 proyectos en clientes. • Experiencia en proyectos de auditorías de cumplimiento de seguridad, avalada por, al menos 3 proyectos en clientes. • Experiencia en la definición de planes de protección en el ámbito LPIC, avalada por, al menos 3 proyectos en clientes. • Experiencia en auditorías de certificación, propias y de clientes, de la UNE-EN ISO/IEC 27001 y del ENS, avalada por, al menos 3 proyectos en clientes. • Experiencia y conocimientos en la realización de Planes de Continuidad de Negocio, avalada por, al menos 2 proyectos en clientes. • Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación del Gobierno de seguridad	Consultor Senior (Gobierno)	1 recurso al 100% de la duración del proyecto
EXPERIENCIA		
<p>Al menos seis (6) años en las actividades ligadas a la línea de actuación de referencia.</p> <p>De los 6 años de experiencia, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Experiencia demostrable y acreditada como consultor en proyectos de adecuación a las normativas normativa y buenas prácticas de seguridad de la información, en particular del ENS e UNE-EN ISO/IEC 27001. Acreditación de haber participado en la realización de planes de protección referidos a la normativa LPIC. Acreditación de haber participado en el diseño y definición cuadros de mando de Gobierno, riesgo y cumplimiento de seguridad de la información. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá disponer de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> Título homologado por el CNP de Director de Seguridad. <p>Al menos una de las siguientes acreditaciones:</p> <ul style="list-style-type: none"> CISM (Certified Information Security Manager) de ISACA. CISA (Certified Information Security Auditor) de ISACA. CISSP (Certified Information Systems Security Professional) de ISC2. Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). En todos los casos deberá estar certificado en la versión vigente de la norma UNE-ISO 27001. 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Conocimientos de la normativa y buenas prácticas de seguridad de la información, especialmente del ENS, UNE-EN ISO/IEC 27001:2023 y normativa LPIC, a través de los respectivos cursos de formación realizados (al menos, 80 horas en cada uno de los tres ámbitos). Conocimiento de herramientas de cuadros de mando. Experiencia en definición de cuadros de mando de seguridad, avalada por, al menos 2 proyectos en clientes. Conocimiento de herramientas de mercado GRC de seguridad de la información. Conocimiento de las herramientas de seguridad del CCN, CNPIC y AEPD. Experiencia en la elaboración de planes directores de seguridad y en la elaboración de normativas y procedimientos de seguridad de la información, avalada por, al menos 2 proyectos en clientes. Experiencia en proyectos de adecuación a la UNE-EN ISO/IEC 27001:2023 y al ENS, avalada por, al menos 2 proyectos en clientes. Experiencia en proyectos de auditorías de cumplimiento de seguridad, avalada por, al menos 2 proyectos en clientes. Experiencia en la definición de planes de protección en el ámbito LPIC, avalada por, al menos 2 proyectos en clientes. Experiencia en auditorías de certificación, propias y de clientes, de la UNE-EN ISO/IEC 27001 y del ENS, avalada por, al menos 2 proyectos en clientes. Experiencia y conocimientos en la realización de Planes de Continuidad de Negocio, avalada por, al menos 2 proyectos en clientes. Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform. Experiencia y participación en proyectos en los que se hayan realizado desarrollos a medida con las soluciones de MS365 y de Microsoft Power Platform. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Dirección y Coordinación de Normativa, Planes y Programas de seguridad	Jefe de Proyecto	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
Al menos seis (6) 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá disponer de la siguiente formación:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Al menos dos certificaciones de entre las siguientes, o formación, en el caso de que se especifique su duración en horas:</p> <ul style="list-style-type: none"> <i>Cybersecurity Fundamentals Certificate (CSX)</i> de ISACA. <i>Certified Data Privacy Solutions Engineer (CDPSE)</i> de ISACA. Máster en Derecho Tecnológico o similar. Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). Auditor Jefe o Implantador Jefe ISO 22301 - Sistema de Gestión de Continuidad del Negocio. 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Liderazgo y coordinación de equipos multidisciplinares de trabajo, planificación, seguimiento y control de actividades en proyectos de oficina de gobierno de seguridad con afectación en el ámbito de marcos normativos de ciberseguridad, seguridad de la información, protección de datos, protección de infraestructuras estratégicas, críticas y servicios esenciales (funciones GRC de Gobierno, Riesgo y Cumplimiento). Identificación de riesgos y emisión de orientaciones sobre diversos estándares y normativas: (RGPD/LOPDGDD, UNE-EN ISO/IEC 27001:2023, ISO 22301, ENS y series CCN-STIC, NIS y NIS2, LPIC, NIS, e informes de buenas prácticas o recomendaciones). Diseño e implementación de sistemas de gestión de seguridad de la información conforme a ISO 27001, 27002, Esquema Nacional de Seguridad (ENS) y controles asociados. Diseño e implementación de planes relacionados con la protección de infraestructuras críticas. Identificación y evaluación de herramientas y tecnologías de seguridad y emisión de recomendaciones sobre su implementación. Diseño e implementación de estrategias de seguridad. Diseño de planes de formación y acciones de concienciación en materia de seguridad de la información. Impartición de acciones formativas y de concienciación. Identificación de requisitos, diseño, coordinación y seguimiento de planes de acción, programas y/o medidas para mejorar la seguridad y medir su eficacia. Asesoramiento legal, seguimiento de normativa y elaboración de disposiciones de carácter general en materia de seguridad. Gestión de incidentes de seguridad y brechas, asesoramiento sobre actividades de contención y respuesta. Interlocución con partes interesadas. Experiencia en proyectos de seguridad de la información en el sector público, avalada, al menos, por 3 proyectos. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Normativa, Planes y Programas de seguridad	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
Al menos cinco (5) años de experiencia como consultor especializado en normativa de seguridad de la información, gestión y desarrollo de proyectos 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá disponer de alguna de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Al menos dos certificaciones de entre las siguientes, o formación, en el caso de que se especifique su duración en horas:</p> <ul style="list-style-type: none"> Cybersecurity Fundamentals Certificate (CSX) de ISACA. Certified Data Privacy Solutions Engineer (CDPSE) de ISACA. Máster en Derecho Tecnológico o similar. Auditor Jefe o Implantador Jefe ISO 22301 - Sistema de Gestión de Continuidad del Negocio. 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Coordinación, desarrollo y ejecución de planes de acción y planes estratégicos de seguridad en proyectos de la naturaleza de una Oficina de Gobierno de Seguridad. Diseño, desarrollo y seguimiento de planes enfocados en la gestión de riesgos, planes estratégicos, tácticos u operativos en el ámbito de la seguridad de la información, garantizando su cumplimiento. Análisis y gestión de riesgos. Metodologías formales de análisis y gestión de riesgos y aplicación práctica de análisis y gestión de riesgos. Cumplimiento del marco de controles de seguridad conforme a los requisitos o requerimientos de auditoría. Operación diaria de gobierno de la seguridad, manteniendo la excelencia operacional y resolviendo problemas e incidencias para mantener la continuidad de las operaciones. Definición, desarrollo y actualización de herramientas de reporte de indicadores y métricas de seguimiento. Verificación del cumplimiento de planes de acción de medidas correctoras derivados de auditorías. Elaboración de políticas, normas, procedimientos e instrucciones técnicas de seguridad de la información y legislación conexas, en cumplimiento de los requisitos legales y normativos, principios y buenas prácticas que sean de aplicación a las competencias de la Agencia. Evaluaciones periódicas de seguimiento del progreso del proyecto a través de indicadores y cuadros de mando. Análisis de informes de auditorías de seguridad (UNE-EN ISO/IEC 27001:2023, 27002 y ENS). Gestión documental de sistemas de gestión de seguridad. Experiencia en proyectos de seguridad de la información en el sector público, avalada, al menos, por 3 proyectos. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Normativa, Planes y Programas de seguridad	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
Al menos cinco (5) años de experiencia como consultor especializado en normativa de seguridad de la información, gestión y desarrollo de proyectos 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá disponer de alguna de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Al menos <u>dos certificaciones</u> de entre las siguientes, o formación, en el caso de que se especifique su duración en horas:</p> <ul style="list-style-type: none"> Cybersecurity Fundamentals Certificate (CSX) de ISACA. Certified Data Privacy Solutions Engineer (CDPSE) de ISACA. Máster en Derecho Tecnológico o similar. Auditor Jefe o Implantador Jefe ISO 22301 - Sistema de Gestión de Continuidad del Negocio. 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Coordinación, desarrollo y ejecución de planes de acción y planes estratégicos de seguridad en proyectos de la naturaleza de una Oficina de Gobierno de Seguridad. Diseño, desarrollo y seguimiento de planes enfocados en la gestión de riesgos, planes estratégicos, tácticos u operativos en el ámbito de la seguridad de la información, garantizando su cumplimiento. Análisis y gestión de riesgos. Metodologías formales de análisis y gestión de riesgos y aplicación práctica de análisis y gestión de riesgos. Cumplimiento del marco de controles de seguridad conforme a los requisitos o requerimientos de auditoría. Operación diaria de gobierno de la seguridad, manteniendo la excelencia operacional y resolviendo problemas e incidencias para mantener la continuidad de las operaciones. Definición, desarrollo y actualización de herramientas de reporte de indicadores y métricas de seguimiento. Verificación del cumplimiento de planes de acción de medidas correctoras derivados de auditorías. Elaboración de políticas, normas, procedimientos e instrucciones técnicas de seguridad de la información y legislación conexas, en cumplimiento de los requisitos legales y normativos, principios y buenas prácticas que sean de aplicación a las competencias de la Agencia. Evaluaciones periódicas de seguimiento del progreso del proyecto a través de indicadores y cuadros de mando. Análisis de informes de auditorías de seguridad (UNE-EN ISO/IEC 27001:2023, 27002 y ENS). Gestión documental de sistemas de gestión de seguridad. Experiencia en proyectos de seguridad de la información en el sector público, avalada, al menos, por 3 proyectos. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Normativa, Planes y Programas de seguridad	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
Al menos cinco (5) 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas o Derecho con formación específica en seguridad de la información y/o ciberseguridad.		
FORMACIÓN COMPLEMENTARIA		
Deberá disponer de alguna de las siguientes acreditaciones de seguridad: <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). Certificado de conformidad con el Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos. Máster o curso superior en Derecho TIC o similar. 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Análisis y resolución de consultas en cuestiones legales sobre seguridad de la información y normativa relacionada. Emisión de informes jurídicos en relación a distintas materias en el ámbito de la seguridad. Elaboración de políticas, normas, procedimientos e instrucciones técnicas de seguridad de la información y legislación conexas, en cumplimiento de los requisitos legales y normativos, principios y buenas prácticas que sean de aplicación a las competencias de la Agencia. Adaptación de políticas y procesos con orientación al cumplimiento en materia de seguridad de la información y ciberseguridad (RGPD/LOPDGDD, UNE-EN ISO/IEC 27001:2023, ENS, NIS y NIS 2). Identificación de amenazas y/o vulnerabilidades y adopción de medidas de seguridad. Colaboración e interlocución con distintas unidades organizativas con afección en ciberseguridad y seguridad de la información. Aplicación de marcos normativos (RGPD/LOPDGDD, UNE-EN ISO/IEC 27001:2023, ENS, NIS, NIS, guías CCNCERT, etc.). Gestión documental de sistemas de gestión de seguridad. Conocimientos en herramientas de GRC de seguridad de la información. Experiencia en proyectos de seguridad de la información en el sector público, avalada, al menos, por 3 proyectos. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Normativa, Planes y Programas de seguridad	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
Al menos cinco (5) 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
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas o Derecho con formación específica en seguridad de la información y/o ciberseguridad...
FORMACION COMPLEMENTARIA
<p>Deberá disponer de alguna de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). Máster o curso superior en Derecho TIC o similar.
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS
<ul style="list-style-type: none"> Diseño y coordinación de proyectos de concienciación en entornos corporativos. Detección de necesidades formativas, teniendo en cuenta las tendencias y el entorno. Desarrollo del programa de concienciación y su plan de acción derivado del análisis de riesgos y el contexto organizativo. Diseño de programas de formación y/o concienciación de ciberseguridad basados en técnicas de ingeniería social. Soporte en la implementación técnica de herramientas de concienciación, soporte y supervisión de campañas y elaboración de la documentación técnica. Diseño de estrategias y acciones de comunicación. Evaluación de indicadores críticos derivados de ejercicios y acciones de concienciación. Identificación de áreas de mejora en simulaciones, respuesta de usuarios o en sesiones de formación. Elaboración y presentación de informes ejecutivos de resultados, evaluación, acciones de mejora y efectividad de las campañas. Identificación de requisitos, diseño, coordinación y seguimiento de planes de acción, programas y/o medidas para mejorar la seguridad y medir su eficacia. Elaboración y gestión de la documentación asociada a campañas de concienciación y/o formación en seguridad. Soporte en la programación de controles de cumplimiento, obtención y archivo de evidencias destinadas a acreditar el cumplimiento y el desarrollo de auditorías. Soporte en la obtención de información y capacidades de comunicación con diferentes unidades organizativas, para comprender las necesidades de manera precisa y acertar en los datos que se proporcionan. Configuración de herramientas de gestión y conservación documental y el mantenimiento de la estructura documental.

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Dirección y Coordinación de Gestión de riesgos y auditoría	Jefe de Proyecto	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
<p>Al menos seis (6) 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.</p> <p>De los 6 años de experiencia mínima como Jefe de Proyecto, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Al menos 2 de ellos han debido desarrollarse en organizaciones del sector público español. Experiencia demostrable de al menos 2 años gestionando proyectos en el ámbito específico de Gestión de riesgos TIC, con la metodología MAGERIT y la herramienta PILAR en el Esquema Nacional de Seguridad y/o la norma UNE-EN ISO/IEC 27001:2023, o en su defecto en la adecuación y/o implantación del Esquema Nacional de Seguridad del sector público. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		

FORMACION COMPLEMENTARIA

Deberá acreditarse:

- Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas).

Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:

- CRISC (Certified in Risk and Information Systems Control) de ISACA.
- Gestión de riesgos en Seguridad de la información según la norma ISO 27005 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).
- Gestión de riesgos en Seguridad de la información según la norma ISO 31000 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).
- Certificación RMP-Risk Management Professional de PMI.

Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:

- CISM (Certified Information Security Manager) de ISACA.
- CISA (Certified Information Security Auditor) de ISACA.
- CISSP (Certified Information Systems Security Professional) de ISC2.
- ISSMP (Information Systems Security Management Professional) de ISC2.
- Certificación en Gestión de proyectos PMP o PRINCE.
- Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).

EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS

- Conocimientos del Esquema Nacional de Seguridad, avalados por cursos de formación de, al menos, 80 horas.
- Conocimientos de la UNE-EN ISO/IEC 27001:2023 y 27002, avalados por cursos de formación de, al menos, 80 h.
- Análisis y Gestión de Riesgos de sistemas de información en el ámbito de normativas de seguridad (ENS, UNE-EN ISO/IEC 27001:2023).
- Experiencia de uso de la metodología MAGERIT y en el uso, diseño y parametrización de riesgos con la herramienta PILAR, avalada por, al menos, 3 proyectos en el sector público.
- Implantación del Esquema Nacional de Seguridad y guías STIC y conocimiento de las herramientas de seguridad del CCN.
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.
- Experiencia en definición de cuadros de mando de seguridad.
- Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform ((List, PowerAutomate, PowerApp, PowerBI, etc...))
- Conocimientos avanzados de herramientas ofimáticas de Microsoft (Excel, Word, powerpoint...)

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Gestión de riesgos y auditoría - 1	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
<p>Al menos cinco (5) años de experiencia en proyectos 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.</p> <p>De los 5 años de experiencia, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Al menos 2 años de experiencia demostrable y acreditada como gestor y analista de riesgos en organizaciones del sector público español con la metodología MAGERIT y la herramienta PILAR en el ámbito del Esquema Nacional de Seguridad y/o UNE-EN ISO/IEC 27001:2023 (al menos 12 meses deben ser obligatoriamente con análisis de riesgos del Esquema Nacional de Seguridad). Acreditación de haber participado en la gestión de riesgos de seguridad de la información, en al menos 2 organizaciones diferentes del sector público español. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:</p> <ul style="list-style-type: none"> CRISC (Certified in Risk and Information Systems Control) de ISACA. Gestión de riesgos en Seguridad de la información según la norma ISO 27005 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...) 		

- Gestión de riesgos en Seguridad de la información según la norma ISO 31000 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...)
 - Certificación RMP-Risk Management Professional de PMI.
- Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:
- CISM (Certified Information Security Manager) de ISACA.
 - CISA (Certified Information Security Auditor) de ISACA.
 - CISSP (Certified Information Systems Security Professional) de ISC2.
 - ISSMP (Information systems Security Management Professional) de ISC2.
 - Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).

EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS

- Conocimientos del Esquema Nacional de Seguridad (RD 311/2022).
- Conocimientos de la UNE-EN ISO/IEC 27001:2023 y 27002.
- Análisis y Gestión de Riesgos de sistemas de información en el ámbito de normativas de seguridad (ENS, UNE-EN ISO/IEC 27001:2023...).
- Experiencia de uso de la metodología MAGERIT y en el uso, diseño y parametrización de riesgos con la herramienta PILAR, avalada por, al menos, 3 proyectos en el sector público.
- Implantación del Esquema Nacional de Seguridad y guías STIC y conocimiento de las herramientas de seguridad del CCN.
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad. Informes de riesgos y planes de tratamiento.
- Conocimientos de arquitectura de software, operación de sistemas, entornos web, bases de datos, metodología de desarrollo seguro, redes, infraestructuras, etc...
- Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform ((List, PowerAutomate, PowerApp, PowerBI, etc...).
- Conocimientos avanzados de herramientas ofimáticas de Microsoft (Excel, Word, powerpoint...)

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Operación de Gestión de riesgos y auditoría - 2	Consultor senior	1 recurso 100% de la duración del proyecto
EXPERIENCIA		
<p>Al menos cinco (5) años de experiencia en proyectos 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.</p> <p>De los 5 años de experiencia, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> • Al menos 2 años de experiencia demostrable y acreditada como gestor y analista de riesgos en organizaciones del sector público español con la metodología MAGERIT y la herramienta PILAR en el ámbito del Esquema Nacional de Seguridad y/o UNE-EN ISO/IEC 27001:2023 (al menos 12 meses deben ser obligatoriamente con análisis de riesgos del Esquema Nacional de Seguridad). • Acreditación de haber participado en la gestión de riesgos de seguridad de la información en al menos 2 clientes del sector público español. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> • Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:</p> <ul style="list-style-type: none"> • CRISC (Certified in Risk and Information Systems Control) de ISACA. • Gestión de riesgos en Seguridad de la información según la norma ISO 27005 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...) • Gestión de riesgos en Seguridad de la información según la norma ISO 31000 (con titulación expedida por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...) • Certificación RMP-Risk Management Professional de PMI. <p>Deberá disponer de al menos una de las siguientes acreditaciones de seguridad en vigor:</p> <ul style="list-style-type: none"> • CISM (Certified Information Security Manager) de ISACA. • CISA (Certified Information Security Auditor) de ISACA. • CISSP (Certified Information Systems Security Professional) de ISC2. 		

- ISSMP (Information systems Security Management Professional) de ISC2.
- Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).

EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS

- Conocimientos del Esquema Nacional de Seguridad (RD 311/2022)-
- Conocimientos de la UNE-EN ISO/IEC 27001:2023 y 27002, avalados por cursos de formación de, al menos, 80 horas.
- Análisis y Gestión de Riesgos de sistemas de información en el ámbito de normativas de seguridad (ENS, UNE-EN ISO/IEC 27001:2023...).
- Experiencia de uso de la metodología MAGERIT y en el uso, diseño y parametrización de riesgos con la herramienta PILAR, avalada por, al menos, 3 proyectos en el sector público.
- Implantación del Esquema Nacional de Seguridad y guías STIC y conocimiento de las herramientas de seguridad del CCN.
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad. Informes de riesgos y planes de tratamiento.
- Conocimientos de arquitectura de software, operación de sistemas, entornos web, bases de datos, metodología de desarrollo seguro, redes, infraestructuras, etc...
- Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform ((List, PowerAutomate, PowerApp, PowerBI, etc...)).
- Conocimientos avanzados de herramientas ofimáticas de Microsoft (Excel, Word, powerpoint...)

Equipo Proyecto (de Cuota Variable): Líneas de actuación y actividades a desarrollar.

Orientación: Implantación de proyectos y desarrollo de servicios a demanda de Madrid Digital.

El equipo proyecto se compondrá de los recursos necesarios que se estimen en cada caso, y que deberán cumplir con carácter de mínimos el perfil profesional requerido para cada proyecto de la OGS. Una vez conformado el equipo de un proyecto concreto, este tendrá dedicación exclusiva para MD, según se determine en el encargo.

Aunque se recoja una amplia relación de conocimientos específicos para cada uno de los perfiles profesionales previstos, consultor senior e ingeniero de seguridad, será en la fase previa de cada uno de los proyectos requeridos y aprobados por MD donde se determinará el conjunto de conocimientos y experiencia específicos que serán necesarios para poder ejecutar adecuadamente los trabajos y, de esta manera, el adjudicatario pueda seleccionar a los recursos que se asignen a cada uno de los perfiles.

Por tanto, el adjudicatario garantizará la disponibilidad de recursos suficientes para que reúnan todos los requisitos de experiencia, titulación, formación complementaria y de conocimientos específicos requeridos en cada perfil

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Gestión de Proyectos o Servicios no planificados	Consultor senior	100% de la duración del proyecto aprobado. 9.600 horas estimadas.
EXPERIENCIA		
Al menos cinco (5) 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
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.
FORMACION COMPLEMENTARIA
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer una de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> CISM (Certified Information Security Manager) de ISACA. CISA (Certified Information Security Auditor) de ISACA. CISSP (Certified Information Systems Security Professional) de ISC2. Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...).
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS
<ul style="list-style-type: none"> Conocimientos de la normativa y buenas prácticas de seguridad de la información, especialmente del ENS, UNE-EN ISO/IEC 27001:2023 y normativa LPIC, avalados por cursos de formación de, al menos, 80 horas. Experiencia en la elaboración de planes directores de seguridad y en la elaboración de normativas y procedimientos de seguridad de la información, avalados por, al menos, 2 proyectos. Conocimiento de herramientas de cuadros de mando. Conocimiento de herramientas de mercado GRC de seguridad de la información. Conocimiento de las herramientas de seguridad del CCN, CNPIC y AEPD. Experiencia en proyectos de adecuación a la UNE-EN ISO/IEC 27001:2023 y al ENS, avalados por, al menos, 2 proyectos. Experiencia en la definición de planes de protección en el ámbito LPIC, avalados por, al menos, 2 proyectos. Amplia experiencia en definición de cuadros de mando de seguridad. Experiencia y conocimientos en la realización de Planes de Continuidad de Negocio. Conocimiento técnico de infraestructuras de sistemas. Conocimiento técnico de infraestructuras de comunicaciones. Conocimiento de infraestructuras y soluciones de seguridad perimetral. Conocimiento técnico de gestión y administración de sistemas (especialmente de directorio Activo, S.O.Windows y Linux, BBDD Oracle). Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform. Experiencia y participación en proyectos en los que se hayan realizado desarrollos a medida con las soluciones de MS365 y de Microsoft Power Platform.

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Gestión de Proyectos o Servicios no planificados	Ingeniero de seguridad	100% de la duración del proyecto aprobado. 11.200 horas estimadas.
EXPERIENCIA		
Al menos cinco (5) 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		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		

FORMACION COMPLEMENTARIA
Deberá acreditarse: <ul style="list-style-type: none">Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas).
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS
<ul style="list-style-type: none">Conocimientos de la normativa y buenas prácticas de seguridad de la información, especialmente del ENS, UNE-EN ISO/IEC 27001:2023 y normativa LPIC, avalados por cursos de formación de, al menos, 80 horas.Experiencia en desarrollo de cuadros de mando de seguridad.Conocimiento técnico de infraestructuras de sistemas.Conocimiento técnico de infraestructuras de comunicaciones.Conocimiento de infraestructuras y soluciones de seguridad perimetral.Conocimiento técnico de gestión y administración de sistemas (especialmente de directorio Activo, S.O.Windows y Linux, BBDD Oracle).Conocimiento de las herramientas de MS365 y de las soluciones de Microsoft Power Platform.Experiencia en proyectos de diseño y desarrollos de portales web y de desarrollos a medida con las soluciones de MS365 y de Microsoft Power Platform.

7.2 LOTE 2: Servicios de auditoría y verificación de cumplimiento de seguridad de la información

El equipo de trabajo de este servicio estará diferenciado por cada uno de los dos dominios definidos en la cláusula 5:

COUTA FIJA:

- Dominio de auditorías de cumplimiento de seguridad de la información:**

El adjudicatario constituirá el equipo de trabajo denominado **Equipo Base de Auditoría** (cuota fija) con las capacidades y perfiles necesarios definidos, que incluirá:

- Prestación del servicio continuo de dirección, coordinación y seguimiento de las auditorías de cumplimiento de seguridad de la información y de las revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información.
- Prestación del servicio continuo en la ejecución de las auditorías definidas para este dominio en la cláusula 5 del presente pliego.

CUOTA VARIABLE:

- Dominio de revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información:**

El adjudicatario constituirá el equipo de trabajo denominado **Equipo de Auditorías Extraordinarias (cuota variable)** con las capacidades y perfiles necesarios definidos, que incluirá:

- Prestación del servicio no planificado (cuota variable), bajo demanda de MD, en la ejecución de las revisiones, verificaciones o diagnósticos de cumplimiento extraordinarias definidas para este dominio en la cláusula 5 del presente pliego.

El número de máximo de horas estimado por categorías para los servicios no planificados (cuota variable), por anualidades es el siguiente:

Revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información (Cuota VARIABLE) - Equipo de auditorías extraordinarias DEDICACIONES por perfiles profesionales			
PERFILES PROFESIONALES	HORAS 2027 (10 meses)	HORAS 2028 (8 meses)	HORAS TOTALES (18 meses)
Auditor Senior	748	660	1.408
Auditor de Seguridad	634	1.902	2.536
Ingeniero de Seguridad	88	264	352
HORAS TOTALES	1.470	2.826	4.296

El Equipo Base de Auditoría se conformará, para el dominio de auditorías de cumplimiento de seguridad de la información, con dedicación exclusiva dos (2) recursos, que deberán cumplir con carácter de mínimos el perfil profesional requerido:

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Auditorías de cumplimiento de seguridad de la información	Auditor senior 1 (Equipo base)	100% durante 15 meses de ejecución del proyecto. Con inicio efectivo de trabajo según determine Madrid Digital.
EXPERIENCIA		
<p>Al menos ocho (8) años de experiencia como auditor senior de seguridad 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.</p> <p>De los 8 años de experiencia mínima como auditor senior, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Experiencia demostrable y acreditada, como Auditor Senior/Auditor Jefe, de al menos 5 auditorías internas o de conformidad del Esquema Nacional de Seguridad de organizaciones del sector público español, en al menos 3 organizaciones diferentes. Experiencia demostrable y acreditada de haber realizado al menos 4 auditorías como auditor senior de la norma ISO 27001 y 27002. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> CISA (Certified Information Security Auditor) de ISACA. Certificación Auditor Líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...). 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Experto en Auditoría del Esquema Nacional de Seguridad en el sector público español. Experto en Auditoría de la norma ISO 27001, con especial importancia en la auditoría de los controles de seguridad aplicables. Conocimiento metodológico en normativas y legislación de seguridad. 		

- Implantación del Esquema Nacional de Seguridad y profundo conocimiento de las guías STIC y herramientas de seguridad del CCN.
- Diseño e implantación de Sistemas de Gestión de Seguridad de la Información, SGSI.
- Propuestas de soluciones y mejoras en materia de seguridad de la información.
- Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad.

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Auditorías de cumplimiento de seguridad de la información	Auditor senior 2 (Equipo base)	100% durante 15 meses de ejecución del proyecto. Con inicio efectivo de trabajo según determine Madrid Digital.
EXPERIENCIA		
<p>Al menos ocho (8) años de experiencia como auditor senior de seguridad 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.</p> <p>De los 8 años de experiencia mínima como auditor senior, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> • Experiencia demostrable y acreditada, como Auditor Senior/Auditor Jefe, de al menos 5 auditorías internas o de conformidad del Esquema Nacional de Seguridad de organizaciones del sector público español, en al menos 3 organizaciones diferentes. • Experiencia demostrable y acreditada de haber realizado al menos 4 auditorías como auditor senior de la norma ISO 27001 y 27002. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> • Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> • CISA (Certified Information Security Auditor) de ISACA. • Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...) 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> • Experto en Auditoría del Esquema Nacional de Seguridad en el sector público español. • Experto en Auditoría de la norma ISO 27001, con especial importancia en la auditoría de los controles de seguridad aplicables. • Conocimiento metodológico en normativas y legislación de seguridad. • Implantación del Esquema Nacional de Seguridad y profundo conocimiento de las guías STIC y herramientas de seguridad del CCN. • Diseño e implantación de Sistemas de Gestión de Seguridad de la Información, SGSI. • Propuestas de soluciones y mejoras en materia de seguridad de la información. • Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad. 		

El **Equipo de Auditorías Extraordinarias** se conformará, para el **dominio de revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información**, de los recursos necesarios que se estimen en cada caso, y que deberán cumplir con carácter de mínimos el perfil

profesional requerido para cada revisión, verificación o diagnóstico requerido. Una vez conformado el equipo de una auditoría concreta, este tendrá dedicación exclusiva para MD, según se determine en el encargo.

Cuando el responsable de Gobierno del Servicio de MD requiera, formalmente y por escrito, al responsable de Gobierno del Servicio del adjudicatario abordar un trabajo variable (revisión, verificación o diagnóstico de cumplimiento de seguridad de la información), antes de 8 días laborables, este último tendrá que enviar a MD una carta de encargo con la propuesta de las condiciones y estimaciones correspondientes. Deberá realizarse una descripción detallada de los objetivos del encargo, de las actividades y tareas a realizar, de los entregables comprometidos, así como la cuantificación del esfuerzo, medido en horas/hombre por cada uno de los perfiles profesionales propuestos. Corresponderá al responsable de Gobierno del Servicio de MD valorar su contenido quedando bajo su discreción incorporar las modificaciones que considere oportunas. En caso de discrepancia, prevalecerá el criterio razonado y documentado del responsable de Gobierno del Servicio de MD, salvo que la desviación sea igual o superior a dos terceras partes de lo estimado por el responsable de Gobierno del Servicio del adjudicatario, caso en el que se elevará al Comité de Seguimiento del Contrato el cual decidirá el criterio en base a los informes razonados de ambas partes.

El retraso en la entrega de la carta de encargo de un proyecto variable más allá del tiempo antes mencionado dará lugar a la penalización correspondiente.

Cuando el responsable de Gobierno del Servicio de MD comunique al responsable de Gobierno del Servicio del adjudicatario la aprobación y necesidad de inicio de un nuevo trabajo del dominio de auditorías extraordinarias conforme a la carta de encargo correspondiente, **antes de 12 días laborables, deberá haberse constituido el equipo de trabajo de auditorías extraordinarias.**

Los equipos de auditoría podrán constituirse en número variable de componentes sobre la base de cualquier combinación de perfiles profesionales contemplados en el pliego.

El adjudicatario estará obligado a poner a disposición de Madrid Digital 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.

Queda bajo el criterio exclusivo de MD realizar los cambios que considere en base a los efectivos disponibles y a los plazos comprometidos por Madrid Digital en cada caso.

Por tanto, el adjudicatario garantizará la disponibilidad de recursos suficientes para que reúnan todos los requisitos de experiencia, titulación, formación complementaria y de conocimientos específicos requeridos en cada perfil.

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información	Auditor senior (Equipo variable)	1.408 horas estimadas.

Los requerimientos de este perfil (Auditor senior-Equipo variable) son los mismos que los ya mencionados anteriormente en los perfiles auditor senior 1 y auditor senior 2 del equipo base. La asignación de la persona al perfil Auditor senior (Equipo variable) corresponderá a una de las dos personas asignadas a los perfiles auditor senior 1 y auditor senior 2 del equipo base.

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información	Auditor de seguridad	2.536 horas estimadas.
EXPERIENCIA		
<p>Al menos seis (6) años de experiencia como auditor senior de seguridad 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.</p> <p>De los 6 años de experiencia mínima como auditor senior, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Experiencia demostrable y acreditada de al menos 2 años completos como Auditor Senior/Auditor Jefe en auditorías internas o de conformidad del Esquema Nacional de Seguridad. Experiencia demostrable y acreditada de haber realizado al menos 1 auditoría como auditor senior de la norma ISO 27001 y 27002. 		
TITULACIÓN		
Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.		
FORMACION COMPLEMENTARIA		
<p>Deberá acreditarse:</p> <ul style="list-style-type: none"> Esquema Nacional de Seguridad (deberá acreditarse un mínimo de 80 horas). <p>Deberá disponer, al menos, una de las siguientes acreditaciones de seguridad:</p> <ul style="list-style-type: none"> CISA (Certified Information Security Auditor) de ISACA. Certificación Auditor líder/Lead Auditor/Auditor Interno en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...)* 		
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS		
<ul style="list-style-type: none"> Experiencia en Auditoría del Esquema Nacional de Seguridad en el sector público español. Experiencia en Auditoría de la norma ISO 27001, con especial importancia en la auditoría de los controles de seguridad aplicables. Conocimiento metodológico en normativas y legislación de seguridad. Implantación del Esquema Nacional de Seguridad y profundo conocimiento de las guías STIC y herramientas de seguridad del CCN. Diseño e implantación de Sistemas de Gestión de Seguridad de la Información, SGSI. Propuestas de soluciones y mejoras en materia de seguridad de la información. Análisis, modificación y desarrollo de documentación, normativa y procedimientos de seguridad. 		

LINEA DE ACTIVIDAD	PERFIL	DEDICACIÓN
Revisiones, verificaciones o diagnósticos de cumplimiento de seguridad de la información	Ingeniero de seguridad	352 horas estimadas.

EXPERIENCIA
<p>Al menos cinco (5) años de experiencia en el sector TIC 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, en Servicios de Consultoría de Negocio o Técnica.</p> <p>De los 5 años de experiencia mínima como auditor, se deben cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> Experiencia demostrable y acreditada de al menos 2 años completos como Auditor en auditorías internas o de conformidad del Esquema Nacional de Seguridad. Experiencia demostrable y acreditada de al menos 2 años en proyectos de consultoría tecnológica, arquitectura de software, diseño y desarrollo de sistemas de información y/o en operación de infraestructuras y sistemas, con conocimiento en diversas tecnologías, lenguajes y bases de datos, con especial relevancia en las siguientes: java, Oracle, directorio Activo, LDAP, Oracle forms, php, Joomla, Drupal, Unix, Windows.
TITULACIÓN
<p>Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente, preferiblemente en Informática, Telecomunicaciones o Matemáticas.</p>
EXPERIENCIA Y CONOCIMIENTOS ESPECÍFICOS
<ul style="list-style-type: none"> Conocimientos de operación de sistemas, entornos web, bases de datos, metodología de desarrollo seguro, redes e infraestructuras TIC. Experiencia de al menos 4 años en proyectos de arquitectura de software, diseño y desarrollo de sistemas de información y/o en operación de infraestructuras y sistemas, con conocimiento en diversas tecnologías, lenguajes y bases de datos, con especial relevancia en las siguientes: java, Oracle, directorio Activo, LDAP, Oracle forms, php, Joomla, Drupal, Unix, Windows.

Para cada uno de los perfiles profesionales previstos, auditor senior, auditor de seguridad e ingeniero de seguridad, será en la fase previa de cada uno de los trabajos requeridos por MD donde se concretará el conjunto de conocimientos específicos que serán necesarios para poder ejecutar adecuadamente cada uno de los trabajos en función de su naturaleza.

7.3 LOTE 3: Servicios de auditoría de certificación de cumplimiento de normas de seguridad de la información

El adjudicatario constituirá el equipo de trabajo denominado **Equipo de Auditorías de certificación**, que incluirá:

- Prestación del servicio no planificado (**CUOTA VARIABLE**), bajo demanda de MD, en la ejecución de las revisiones, verificaciones o diagnósticos de cumplimiento extraordinarias definidas para este dominio en la cláusula 6.
- Prestación de cursos de formación en materia de seguridad de la información relacionadas con las certificaciones de cumplimiento del ENS y UNE-ISO 27001:2023 así como en normativas de seguridad de cumplimiento obligatorio para la Agencia, como la NIS 2.

El número máximo de horas estimado para los servicios no planificados de certificación (cuota variable), por anualidades es el siguiente:

Auditoría de certificación de cumplimiento de normas de seguridad de la información (Cuota VARIABLE) - Equipo de auditorías de certificación DEDICACIONES por perfiles profesionales

PERFILES PROFESIONALES	HORAS 2025 (4 meses)	HORAS 2026 (12 meses)	HORAS 2027 (12 meses)	HORAS 2028 (8 meses)	HORAS TOTALES (36 meses)
Auditor (Consultor)	40	280	280	120	720

7.4 **TECNOLOGÍAS Y HERRAMIENTAS**

Con carácter general para los LOTES 1 y 2:

El adjudicatario deberá disponer de las herramientas software que sean necesarias para la adecuada prestación de los servicios descritos en la cláusula 4 del pliego.

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 Madrid Digital. El adjudicatario aportará a su costa las licencias SW necesarias para el funcionamiento de las mismas.

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

- Una plataforma de concienciación de seguridad con capacidad de generar ejercicios y simulaciones con los usuarios finales.
- Una plataforma de generación y edición de documentación gráfica.
- Una plataforma de generación y edición de contenidos audiovisuales.

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

Madrid Digital podrá exigir al adjudicatario, a la finalización del contrato la migración de todos los contenidos documentales desarrollados por la OGS (1) a plataformas propias de forma que todos los contenidos sean accesibles y legibles. El coste asociado al traspaso de información o de las integraciones que tuvieran que realizarse será siempre por cuenta del adjudicatario.

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.

Todo el software aportado por el adjudicatario deberá cumplir con la normativa de seguridad de Madrid Digital y, en caso de tratarse de un producto de seguridad TIC, deberá estar incluido en el catálogo del CCN de Productos de Seguridad de las Tecnologías de la Información y la Comunicación.

Particularidades relativas al LOTE 1:

El adjudicatario asumirá, sin coste adicional para Madrid Digital, el uso de aquellas herramientas o productos comerciales que sean necesarias para la realización de los trabajos, tanto del equipo

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

base como del equipo proyecto. En cualquier caso, estas herramientas o productos comerciales deberán estar directamente relacionadas con la naturaleza de los servicios y trabajos descritos en este pliego.

Los cometidos y las actividades a desarrollar por cada equipo de los proyectos variables 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 las cartas de encargo, el nivel de desarrollo de las capacidades de gestión de la seguridad para Madrid Digital, el modo de prestación y el nivel de calidad de los servicios será marcada por los responsables del Gobierno del Servicio en el marco del Comité de Seguimiento del Contrato.

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.

CLÁUSULA 8. MODELO DE GESTIÓN

8.1 HORARIO Y LUGAR DE PRESTACIÓN DE LOS SERVICIOS

Los servicios objeto del presente pliego siguen el calendario laborable de Madrid Digital. El horario de este servicio será con carácter general de 8x5 en la franja horaria de lunes a viernes de 9:00 h a 18:00 h, los días laborables.

El lugar de prestación de los servicios será habitualmente en las dependencias del adjudicatario, si bien el equipo estará en disposición de personarse en las dependencias de Madrid Digital, si así lo estimase el responsable de los servicios de MD y durante el tiempo que estime necesario.

Todos los gastos ocasionados por los desplazamientos y estancia del personal del contratista durante el cumplimiento del contrato están incluidos en el importe del mismo. Madrid Digital no aceptará costes adicionales por tales causas, que deberán ser asumidos siempre por el contratista.

8.2 DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

La prestación de los servicios solicitados en el presente pliego (3 LOTES) precisa de un adecuado seguimiento en su desarrollo por parte de Madrid Digital. Con objeto de garantizar la correcta ejecución de los mismos y el cumplimiento de los objetivos del proyecto se establecen, para cada lote, la siguiente estructura de Comités de gobierno y seguimiento del servicio.

Para todos los lotes 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.

Las funciones del Comité definido a nivel estratégico son:

- Monitorizar el avance global de los servicios.
- Aprobar los cambios propuestos en el seno de los Comités Técnicos y Operativos 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 CSC.

- 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 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.
- **Nivel operativo:** orientado al gobierno de la operación de los servicios y a su adecuada ejecución, así como al seguimiento, control y aseguramiento de los recursos y esfuerzos necesarios para su correcta ejecución.

Las funciones del Comité definido a nivel operativo son:

- 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.
- Informar y proponer al Responsable de gobierno y seguimiento de la operación del servicio la aplicación de posibles penalizaciones por incumplimientos de los ANS.
- Proponer la realización de proyectos, desarrollo de servicios a demanda o de auditorías o revisiones extraordinarias. La aprobación final de los mismos se realizará en el CTO de gobierno y seguimiento de la operación del servicio que se determine en cada lote.
- 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 Madrid Digital. 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.

Para todos los Comités (CSC y CTO), el adjudicatario deberá elaborar y enviar, 48 horas antes de la celebración de un Comité, la agenda con el orden de los puntos a tratar. Madrid Digital podrá modificar su contenido hasta 24 horas antes de la celebración del Comité y el adjudicatario deberá adaptar la documentación preparada para el Comité a los cambios indicados.

La periodicidad de la celebración de cada Comité, en cada uno de los lotes, se determinará por el responsable del servicio de MD al inicio del contrato.

8.2.1 LOTE 1: Servicios de la Oficina de Gobierno de Seguridad (OGS)

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 de gobierno y operación de los servicios (CTO).
 - CTO de gobierno y seguimiento de la operación del servicio.
 - CTO de seguimiento de la operación de gestión de normativa, planes y programas de seguridad de la información.
 - CTO de seguimiento de la operación de auditoría y gestión de riesgos de seguridad.

Una vez iniciada la ejecución del contrato, se procederá al nombramiento de ambos Comités, de Seguimiento del Contrato 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 Madrid Digital:

El Director del Proyecto (y, por tanto, responsable último en Madrid Digital del funcionamiento de la OGS), que será el titular de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad (SGCPDP), o persona en quien delegue esta función, denominado también **Responsable del Contrato** por parte de Madrid Digital.

El Responsable de gobierno del servicio de Madrid Digital, que será el titular del Área del Área de Gobierno, Riesgo y Cumplimiento de la Seguridad de la información.

Los Responsables Operativos de las líneas de servicio, que serán el titular de la Unidad de normativa, planes y programas de seguridad de la información y el titular de la Unidad de auditoría y gestión de riesgos de seguridad, o personas en quien deleguen esta función.

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 Madrid Digital
- El Responsable de gobierno del servicio
- Por el adjudicatario:
 - El Responsable del Servicio

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.

El CSC celebrará sus reuniones bien en remoto o en las propias dependencias de Madrid Digital, según determine MD, y se realizará con una periodicidad trimestral.

Se levantará acta de cada una de las reuniones del CSC. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en los dos días laborables siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva.

Comités Técnicos y Operativos (CTO)

Su principal objetivo será el seguimiento de la implantación y explotación de los servicios. Se formalizarán los siguientes CTOs y estarán formados por las siguientes personas:

CTO de gobierno y seguimiento de la operación del servicio:

- Por Madrid Digital:
 - El Responsable de gobierno y seguimiento de la operación del servicio
- Por el adjudicatario:
 - El Responsable del servicio

Ocasionalmente, el Comité podrá incorporar a sus sesiones a los Responsables Operativos de las líneas de servicio, 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.

CTO de seguimiento de la operación de gestión de normativa, planes y programas de seguridad de la información.

- Por Madrid Digital:
 - El Responsable Operativo de las líneas de servicio de normativa, planes y programas de seguridad de la información
- Por el adjudicatario:
 - El Responsable del servicio
 - El Responsable de las líneas de servicio de normativa, planes y programas de seguridad de la información de la OGS

CTO de seguimiento de la operación de auditoría y gestión de riesgos de seguridad.

- Por Madrid Digital:
 - El Responsable Operativo de las líneas de servicio de la Unidad de auditoría y gestión de riesgos de seguridad

- Por el adjudicatario:
 - El Responsable del servicio
 - El Responsable de las líneas de servicio de auditoría y gestión de riesgos de seguridad

En cualquiera de los dos últimos CTOs, ocasionalmente, el comité podrá incorporar a sus sesiones al Responsable de gobierno y seguimiento de la operación del servicio de MD y al personal asesor o técnico que se considere necesario, a juicio de cualquiera de las partes. Ninguna de estas personas figurará como miembro permanente del mismo.

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 los dos días laborables siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y a presentación del acta definitiva.

8.2.2 LOTE 2: Servicios de auditoría y verificación de cumplimiento de seguridad de la información

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 de gobierno y operación de los servicios (CTO).

Una vez iniciada la ejecución del contrato, se procederá al nombramiento de ambos Comités, de Seguimiento del Contrato 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 Madrid Digital:

El Director del Proyecto (y, por tanto, responsable último en Madrid Digital del funcionamiento de la OGS), que será el titular de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad, o persona en quien delegue esta función, denominado también Responsable del Contrato por parte de Madrid Digital.

El Responsable de gobierno del servicio de Madrid Digital, que será el titular del Área del Área de Gobierno, Riesgo y Cumplimiento de la Seguridad de la información.

El Responsable operativo del servicio, que serán el titular de la Unidad de auditorías y gestión de riesgos de seguridad, o personas en quien deleguen esta función.

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 Madrid Digital
 - El Responsable de gobierno y seguimiento de la operación del servicio
- Por el adjudicatario:
 - El Responsable del servicio

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.

El CSC celebrará sus reuniones bien en remoto o en las propias dependencias de Madrid Digital, según determine MD, y se realizará con una periodicidad trimestral.

Se levantará acta de cada una de las reuniones del CSC. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en los dos días laborables 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.

Comité Técnico y Operativo (CTO).

Su principal objetivo será el seguimiento de la implantación y explotación de los servicios. Estará formado por las siguientes personas:

- Por Madrid Digital:
 - El Responsable de gobierno del servicio
 - El Responsable Operativo de las líneas de servicio de la Unidad de auditoría y gestión de riesgos de seguridad
- Por el adjudicatario:
 - El Responsable del servicio

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

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 los dos días laborables siguientes a la finalización del Comité, la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y a presentación del acta definitiva.

8.2.3 LOTE 3: Servicios de auditoría de certificación de cumplimiento de normas de seguridad de la información

Se establecerá un único Comité para realizar el control de los trabajos y la toma de decisiones, el Comité de Seguimiento del Contrato (CSC).

Una vez iniciada la ejecución del contrato, se procederá a su nombramiento. A estos efectos se definen las siguientes figuras por parte de Madrid Digital:

El Director del Proyecto (y, por tanto, responsable último en Madrid Digital del funcionamiento de la OGS), que será el titular de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad, o persona en quien delegue esta función, denominado también Responsable del Contrato por parte de Madrid Digital.

El Responsable de gobierno y seguimiento del servicio, que será el titular del Área de Gobierno, Riesgo y Cumplimiento de la Seguridad de la información.

El Responsable operativo del servicio, que serán el titular de la Unidad de auditorías y gestión de riesgos de seguridad, o personas en quien deleguen esta función.

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

- Por Madrid Digital:
 - El Director del Proyecto de Madrid Digital.
 - El Responsable de gobierno y seguimiento del servicio.
 - El Responsable operativo del servicio.
- Por el adjudicatario:
 - El Responsable del servicio.

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.

El CSC celebrará sus reuniones bien en remoto o en las propias dependencias de Madrid Digital, según determine MD, y se realizará con una periodicidad trimestral.

Se levantará acta de cada una de las reuniones del CSC. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en los dos días laborables 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.

8.3 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 la **cláusula 7 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.

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.

Para los LOTES 1 y 2, 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 a los Equipos Base, siguiendo el modelo definido en el **MODELO DE CURRÍCULUM**, que detalle sus datos profesionales (categoría, titulación, formación, actividad profesional, y experiencia y conocimientos específicos), así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos Currículos.

Cada uno de los requisitos mínimos solicitados deberán disponerse en la fecha final de presentación de ofertas.

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.

8.3.1 Requisitos para acceso remoto de proveedores

El servicio de conectividad entre la empresa adjudicataria y la Comunidad de Madrid se considerará incluido dentro del servicio prestado por el adjudicatario y seguirá las siguientes premisas:

- El adjudicatario será responsable de dar adecuada conectividad a sus trabajadores para poder ejecutar el contrato, esto incluye las necesidades de conexión a internet, acceso a correo electrónico, aplicaciones corporativas, accesos VPN, etc.
- El adjudicatario realizará los controles necesarios para asegurar que los accesos a través de su línea de comunicaciones a los CPDs de la Comunidad de Madrid son realizados por los usuarios y máquinas debidamente autorizados.
- En consecuencia, el adjudicatario deberá proporcionar un acceso seguro a su propia red (VPN, extensión de VLAN etc.), de manera que, a los efectos de acceso a los recursos situados en los CPD de la Comunidad de Madrid, cualquier tipo de empleado que se conecte, por cualquier medio y desde cualquier ubicación, aparezca como un usuario del equipo de trabajo y con un direccionamiento IP compatible con el rango reservado por Madrid Digital al contrato del adjudicatario.
- Los trabajadores del adjudicatario que presten sus servicios en edificios de la Comunidad de Madrid no estarán directamente conectados a la red corporativa, sino que, de forma lógica, se encontrarán en un segmento de red que se considera una extensión de la red de su empresa.
- Independientemente de la ubicación de los empleados del adjudicatario, para el acceso lógico a los distintos entornos de la Comunidad objeto del contrato usarán el servicio de conectividad descrito en este apartado.
- Los usuarios que trabajen en las instalaciones de la Comunidad de Madrid dispondrán de un direccionamiento IP en una red diferenciada, asignado por Madrid Digital.
- El adjudicatario debe ofrecer directamente a sus empleados desplazados en sedes de la Comunidad de Madrid los siguientes servicios mínimos, para los que Madrid Digital asignará otro rango IP diferenciado:
 - Servicio de nombres (DNS), en el caso de que los trabajadores en las instalaciones de Madrid Digital deban acceder a servicios locales a su empresa. Este servicio de nombres servirá para acceder a los recursos ubicados en los CPD de la Madrid Digital o a los servicios digitales ofrecidos por su empresa. Para ello, la empresa deberá proporcionar servidores de nombres (DNS), bien haciendo forwarding DNS para los dominios que Madrid Digital determine (si el direccionamiento es compatible con el de la red de la empresa), bien publicando dichos nombres en la red interna mediante técnicas de NAT. En el caso de que no sea preciso acceder por nombre a servicios de su empresa, los puestos de trabajo del adjudicatario podrán utilizar los servidores DNS proporcionados por Madrid Digital.
 - Proxy de navegación a internet, con el fin de que puedan acceder a internet a través de la conectividad entre el CPD de Madrid Digital y las instalaciones del adjudicatario.
 - Servicio de correo electrónico, vía webmail u otras direcciones IP del rango reservado.
- El adjudicatario pondrá en marcha una conexión dedicada desde su empresa a CPDs de la Comunidad de Madrid, contratada y sufragada por la empresa adjudicataria. La comunicación podrá realizarse mediante línea punto a punto o RPV-IP sobre red de operador, siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en los CPDs de la Comunidad de Madrid se

instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.

- La compatibilidad de direccionamiento (mediante NAT), si fuera necesaria, se realizará en los equipos del adjudicatario que empiezan y terminan la línea dedicada.
- Para la conexión de personal externo desde sedes de la Comunidad de Madrid a sistemas de información de la Comunidad o a su propia empresa, el adjudicatario deberá instalar, a su cargo, una conexión dedicada en configuración de alta disponibilidad (doble línea, doble equipo) desde la empresa prestadora a cada una de las sedes de la Comunidad de Madrid. Al igual que en el caso de la conexión con el CPD, la comunicación puede realizarse mediante línea punto a punto o RPV-IP sobre red de operador siempre que garantice que los datos que transiten por dicha conexión no son accesibles por terceros. En consecuencia, en las sedes de la Comunidad de Madrid se instalarán dos equipos ajenos a Madrid Digital, que entregarán el tráfico a/desde la empresa adjudicataria en interfaces Ethernet en los conmutadores de red de Madrid Digital.
- Caudales de la conexión con la empresa: el necesario en cada sentido para la prestación de los servicios objetos del contrato.
- En consecuencia, los trabajadores de la empresa prestataria, ya estén ubicados en instalaciones de la misma o en instalaciones de la Comunidad de Madrid, se conectarán siempre a través de un punto de entrega en un CPD de la Comunidad de Madrid, desde donde podrá acceder a los sistemas de información necesarios para realizar su trabajo.
- La responsabilidad de Madrid Digital con este equipo es:
 - Ofrecer la conectividad física de los equipos a los conmutadores LAN de la sede de la Comunidad de Madrid objeto del contrato para poder alcanzar al router de salida del adjudicatario que conecta con la sede de su empresa (ya sea mediante una línea dedicada o mediante un servicio RPV-IP contratado por dicha empresa).
 - Servicio de DHCP para asignar a cada puesto de trabajo del Adjudicatario en la sede de la Comunidad de Madrid objeto del contrato una dirección IP dentro del rango reservado al Adjudicatario. En su caso, la empresa adjudicataria deberá informar de los servidores DNS que desea que se entreguen a estos puestos.

8.3.2 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 **ACUERDOS DE NIVEL DE SERVICIO**.

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

8.3.3 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 laborables**, 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 cada obligación dará lugar a la correspondiente penalización.

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

8.3.4 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.

CLÁUSULA 9. FORMACIÓN PARA EMPLEADOS DE MADRID DIGITAL

Con relación a la formación incluida en este Pliego, se atenderá a las directrices establecidas por la Dirección competente en esta materia en Madrid Digital. A este respecto, indicar que la dirección competente ha de regirse por un Sistema de Gestión de Calidad basado en la norma ISO 9000-2015 tal y como establece su Convenio Colectivo y que, naturalmente, se audita.

Entre las características más destacables de la formación en Madrid Digital, cabe destacar los siguientes aspectos:

Siempre que exista una Certificación Oficial acorde con la materia de la formación, se priorizará este tipo de formación sobre cualquier otra (ya sea producto, metodología, servicio, etc.). Esta formación ha de incluir el examen de Certificación, que servirá como prueba objetiva que acredite el conocimiento del alumno. En el caso que las Certificaciones caduquen, se pondrá a disposición

de los empleados de Madrid Digital su actualización, bien sea a través de acciones formativas, examen de Certificación, etc.

En el caso que el examen de Certificación esté disponible únicamente en idioma inglés (u otro idioma distinto al español), el proveedor deberá facilitar, uno de similar dificultad, metodología y características que el oficial de Certificación en idioma español. En este último caso, dicha prueba será elaborada y evaluada por un tercero externo e independiente a la empresa suministradora del servicio, de tal manera que se garantice la independencia de la evaluación.

En caso que la materia formativa no tuviera una Certificación asociada, la prueba de la evaluación del conocimiento, al igual que en el caso anterior, será elaborada y evaluada por un tercero externo e independiente a la empresa suministradora del servicio, de tal manera que se garantice la independencia de la evaluación.

Asimismo, la metodología de la formación será asíncrona, siempre que la materia lo permita. De esta manera, el proveedor facilitará los materiales y medios adecuados para la adquisición de los conocimientos a través de esta metodología (vídeos, documentación, gamificación, pruebas parciales, etc.).

Por último, es necesario que se informe del concreto coste de la formación, incluyendo las Certificaciones y tasas de exámenes, a la dirección competente en materia de formación interna en MD.

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

LOTES 1 y 3:

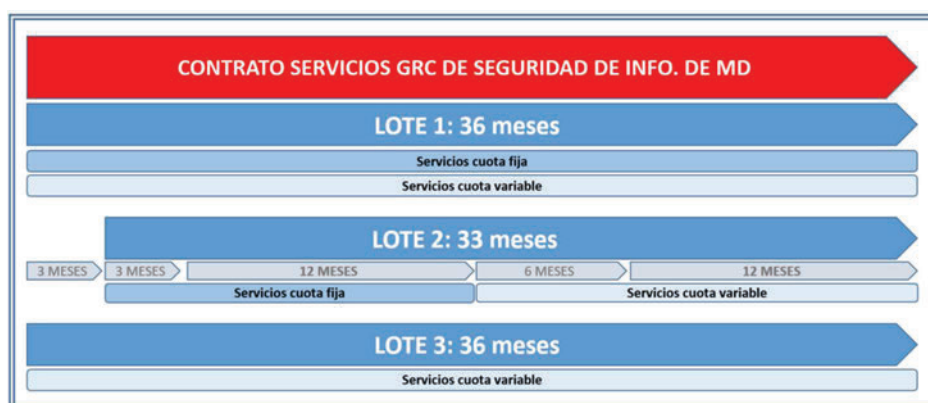
El plazo de ejecución del contrato será de **TREINTA Y SEIS MESES**. A efectos del cálculo del presupuesto y la distribución del importe por anualidades, se ha estimado como fecha de inicio el **1 de septiembre de 2025**

LOTE 2:

El plazo de ejecución del contrato será de **TREINTA Y TRES MESES**. A efectos del cálculo del presupuesto y la distribución del importe por anualidades, se ha estimado como fecha de inicio el **1 de diciembre de 2025**.

- **Servicios de Cuota Fija:** El plazo de ejecución de esta etapa será de **QUINCE MESES** comprendidos desde el inicio del contrato.
 - Durante esta etapa se realizará la planificación de las auditorías hará entrega de los programas de auditoría, El plazo de ejecución de esta etapa será de **TRES MESES** comprendidos desde el inicio del contrato.

- Finalizada la etapa anterior, se realizarán auditorías de controles transversales, y se entregarán los informes de auditoría con la presentación de resultados. El plazo de ejecución de esta etapa será de **DOCE MESES** desde la finalización de la etapa anterior.
- **Servicios de Cuota Variable:** El plazo de ejecución de esta etapa será de **DIECIOCHO MESES** desde la finalización de la última etapa de los servicios de cuota fija.
 - Comprendida la etapa de **Corrección de hallazgos por parte de MD**, y el correspondiente **soporte por parte del equipo auditor:** El plazo de ejecución de esta etapa será de **SEIS MESES** desde la finalización de la última etapa de los servicios de cuota fija.
 - Finalizada la etapa de Corrección de hallazgos por parte de MD, durante esta etapa se hará entrega del informe de verificación de la implantación de medidas y presentación de resultados, y de los informes de auditorías extraordinarias y presentación de resultados. El plazo de ejecución de esta etapa será de **DOCE MESES** desde la finalización de la etapa anterior.



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

Y cualquier otra actividad que Madrid Digital 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.

CLÁUSULA 12. 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 Ciberseguridad, Protección de Datos y Privacidad
Área de Gobierno, Riesgo y Cumplimiento, Protección de Datos y Privacidad
(GRC de seguridad de la información)
E-mail: seguridad_de_la_informacion@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 el Pliego de Cláusulas Administrativas Particulares.

La Subdirectora General de Ciberseguridad, Protección de Datos y Privacidad

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2025 05 14 10:54

Fdo.: Esther Muñoz Fuentes

ANEXO I. MODELO DE CURRÍCULUM

MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO

(A aportar para cada miembro del equipo propuesto)

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

La autenticidad de este documento se puede compro
https://gestiona.comunidad.madrid/csv
mediante el siguiente código seguro de verificación:

Para los LOTES 1 y 2, la 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.

Cada uno de los requisitos mínimos solicitados deberán disponerse en la fecha final de presentación de ofertas

