

Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original

Pliego de Cláusulas Técnicas que han de regir el contrato de servicio denominado **“SOPORTE A LA OFICINA DE GOBIERNO, RIESGO Y CUMPLIMIENTO DE LA AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID”** a adjudicar mediante procedimiento abierto con pluralidad de criterios

Expediente: **AC-001-2025**



INDICE:

CLÁUSULA 1.- INTRODUCCIÓN.....	5
1.1 Contexto normativo y estratégico.....	5
1.1.1 Necesidad y justificación.....	5
1.1.2 Marco normativo y estándares aplicables.....	6
1.1.3 Rol estratégico de la Oficina de GRC.....	6
1.1.4 Consolidación de la ciberseguridad en la Comunidad de Madrid.....	7
1.2 Objetivos del contrato.....	7
CLÁUSULA 2.- OBJETO Y ALCANCE DEL CONTRATO	8
2.1 Descripción general de los servicios requeridos.....	8
2.2 Ámbito de aplicación y alcance funcional.....	9
CLÁUSULA 3.- REQUISITOS GENERALES	10
3.1 Requisitos básicos.....	10
3.1.1 Requisitos técnicos.....	10
3.1.2 Requisitos operativos y de gestión.....	10
3.1.3 Requisitos de comunicación y soporte.....	11
3.2 Cumplimiento de normativa específica.....	11
3.2.1 Normativa aplicable.....	11
3.2.2 Recomendaciones técnicas.....	11
3.2.3 Controles específicos del proceso de adecuación normativa.....	12
CLÁUSULA 4.- CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR	12
4.1 Capacidades clave de la Oficina de GRC.....	12
4.1.1 Implementación y cumplimiento normativo.....	12
4.1.2 Gestión integral de riesgos.....	13
4.1.3 Desarrollo de capacidades y mejora continua.....	13
4.2 Servicios detallados por ámbito.....	13
4.2.1 Apoyo en la implementación de marcos normativos.....	13
4.2.2 Gestión integral de riesgos.....	14
4.2.3 Supervisión de controles técnicos y organizativos.....	14
4.2.4 Formación y sensibilización.....	14
4.2.5 Generación de informes y recomendaciones.....	14
4.2.6 Alineación estratégica con la Agencia.....	14
CLÁUSULA 5.- EQUIPO DE TRABAJO.....	15
5.1 Perfiles requeridos.....	15
5.1.1 Perfiles y responsabilidades clave.....	15
5.2 Requisitos de formación y experiencia.....	16
5.2.1 Responsable de Servicio.....	16
5.2.2 Arquitecto de Seguridad.....	17
5.2.3 Consultor Senior GRC - Especialista Técnico.....	18
5.2.4 Consultor Mid Senior GRC - Ámbito Compliance Legal.....	19
5.2.5 Analista de Seguridad.....	19

5.2.6	Requisitos generales adicionales para todo el equipo	20
5.3	Cambios en el equipo a solicitud de la Agencia.....	20
5.3.1	Supuestos para solicitar cambios en el equipo	20
5.3.2	Procedimiento para solicitar cambios en el equipo	21
5.3.3	Requisitos para la incorporación de nuevos perfiles	21
5.4	Obligación de desempeño en las instalaciones de la Agencia.....	21
CLÁUSULA 6.- TECNOLOGÍAS Y HERRAMIENTAS A UTILIZAR		22
6.1	Herramientas para la gestión del contrato, recursos y servicio prestado.....	22
6.2	Herramientas específicas de gestión GRC	23
CLÁUSULA 7.- MODELO DE GESTIÓN DEL SERVICIO.....		24
7.1	Planificación y seguimiento del servicio	24
7.1.1	Fases del servicio	24
7.1.2	Modo de relación entre adjudicatario y Agencia.....	25
7.2	Acuerdos de nivel de servicio (SLA) y penalizaciones	26
7.2.1	Cumplimiento de plazos	26
7.2.2	Calidad de los entregables.....	26
7.2.3	Disponibilidad del equipo y cumplimiento de dedicación	27
CLÁUSULA 8.- CONTENIDO DE LAS OFERTAS.....		27
8.1	Documentación administrativa.....	27
8.2	Contenido de la oferta relativo a criterios valorables mediante juicio de valor	27
8.2.1	Requisitos de redacción.....	27
8.2.2	Estructura de la oferta.....	27
8.3	Contenido de la oferta relativo a criterios valorables mediante la aplicación de fórmulas	28
CLÁUSULA 9.- GESTIÓN DE LA SEGURIDAD		29
9.1	Cumplimiento de normativas.....	29
9.2	Tratamiento de datos personales.....	29
9.3	Confidencialidad	29
CLÁUSULA 10.- DERECHOS Y OBLIGACIONES		30
10.1	Propiedad de los trabajos realizados	30
10.2	Derechos sobre herramientas y software desarrollado.....	31
CLÁUSULA 11.- CALIDAD DEL SERVICIO.....		31
11.1	Mecanismos de revisión y mejora continua	31
11.2	Evaluación de la satisfacción del cliente	32
CLÁUSULA 12.- PLAZOS, DURACIÓN Y ETAPAS DE LA PRESTACIÓN		33
12.1	Cronograma general	33
12.1.1	Fase de establecimiento inicial	33
12.1.2	Fase de servicio estabilizado	33
12.1.3	Fase de transferencia del servicio.....	33
12.2	Hitos clave	34
12.2.1	Hito 'Entrega de documentos iniciales de planificación, mes 1'	34
12.2.2	Hitos 'Presentación de informe trimestral de avance, final de cada trimestre'	34
12.2.3	Hito 'Reedición del programa anual de implantación de marcos normativos, noviembre de 2025'	34

12.2.4	Hito 'Primer Informe Anual Consolidado, mes 12'	34
12.2.5	Hito 'Reedición del programa anual de implantación de marcos normativos, noviembre de 2026'	34
12.2.6	Hito 'Reedición del programa anual de implantación de marcos normativos, noviembre de 2027'	35
12.2.7	Hito 'Transferencia del servicio'	35
CLÁUSULA 13.- GARANTÍA DE LOS TRABAJOS		35
CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO TÉCNICO		35

CLÁUSULA 1.- INTRODUCCIÓN

1.1 Contexto normativo y estratégico

La Agencia de Ciberseguridad de la Comunidad de Madrid, creada mediante la **Ley 14/2023**, es el organismo instrumental encargado de liderar la estrategia regional en materia de ciberseguridad. Su labor se centra en **coordinar, supervisar y facilitar** la adopción de medidas de protección en la Administración regional, organismos públicos y entidades locales. En adelante, se denominará **Agencia de Ciberseguridad** o simplemente **Agencia**.

Dentro del mandato de la Agencia para liderar esta estrategia regional, la **Oficina de Gobierno, Riesgo y Cumplimiento (GRC)** desempeña un papel fundamental, garantizando un enfoque integral en la **gestión de la seguridad de la información** y en el **cumplimiento de los marcos normativos aplicables**.

El presente contrato se enmarca dentro de esta estrategia, con el objetivo de **fortalecer la gobernanza, la gestión de riesgos y el cumplimiento normativo** en materia de **ciberseguridad y protección de datos**. Se dirige especialmente a las **entidades locales de la Comunidad de Madrid**, priorizando aquellas con **menos de 20.000 habitantes**, que presentan mayores limitaciones de recursos técnicos y organizativos para abordar estos desafíos de forma autónoma.

1.1.1 Necesidad y justificación

La correcta implementación de normativas y estándares internacionales requiere del soporte de especialistas que aseguren un **enfoque estratégico alineado** con los objetivos de la Agencia y las necesidades específicas de las entidades locales. Este contrato responde a las siguientes necesidades clave:

- **Cumplimiento normativo:** Garantizar que las entidades locales **adopten e implementen** el **Esquema Nacional de Seguridad (ENS)**, la **Directiva NIS2**, el **Reglamento General de Protección de Datos (RGPD)** y la **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)**. Esto implica el diseño de **procedimientos internos**, la implantación de **controles adecuados** y la ejecución de **revisiones periódicas** para verificar su efectividad.
- **Gestión integral de riesgos:** **Identificar, analizar y priorizar** los riesgos de ciberseguridad que afectan a los **servicios esenciales y activos críticos** de las entidades locales, proponiendo **planes de mitigación efectivos** basados en su criticidad e impacto potencial.
- **Mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI):** Asegurar la **operatividad y mejora continua** del SGSI de la Comunidad de Madrid, y los complementarios de las entidades locales, conforme a las **exigencias del ENS y estándares internacionales como ISO/IEC 27001 e ISO 22301**, garantizando su **adaptabilidad a los recursos y capacidades de cada entidad local**.
- **Soporte técnico y asesoramiento:** Proporcionar asistencia experta en la definición e implementación de **políticas, normativas internas y planes de actuación en materia de ciberseguridad**, ofreciendo directrices prácticas para facilitar la adopción de medidas efectivas.
- **Homogeneidad en la aplicación normativa:** Fomentar un **enfoque estandarizado**, asegurando **coherencia y uniformidad** en la implementación de normativas de ciberseguridad y evitando discrepancias en los procedimientos aplicados por las entidades locales.
- **Optimización de recursos:** Proveer un **soporte centralizado** que **reduzca la carga administrativa y técnica** de las entidades locales, optimizando el uso de recursos y evitando duplicidades en las iniciativas de ciberseguridad.

- **Fomento de una cultura de ciberseguridad:** Promover acciones de **formación y sensibilización** en el ámbito del Gobierno, Riesgo y Cumplimiento, dirigidas al **personal técnico, responsables de ciberseguridad y cargos electos**, para impulsar la adopción de **buenas prácticas y un enfoque proactivo** frente a las amenazas.
- **Seguimiento y mejora continua:** Realizar **evaluaciones periódicas** que permitan **identificar áreas de mejora**, fomentar la adopción de **lecciones aprendidas** y generar **informes detallados** que refuercen la **madurez en ciberseguridad** de las entidades locales.

1.1.2 Marco normativo y estándares aplicables

La ejecución de este contrato se rige por los siguientes **marcos normativos y estándares internacionales**:

- **Esquema Nacional de Seguridad (ENS):** Garantiza la protección de sistemas y servicios esenciales mediante la aplicación de **controles mínimos obligatorios** definidos en el **Real Decreto 311/2022**.
- **Directiva NIS2 (Directiva (UE) 2022/2555) y normativa derivada:** Refuerza la **resiliencia de operadores esenciales y proveedores digitales**, estableciendo requisitos en **medidas organizativas, técnicas y de notificación de incidentes**. Su transposición al ordenamiento jurídico español se desarrolla a través del **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, junto con las **normativas sectoriales complementarias** necesarias para su aplicación efectiva.
- **Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD):** Establecen las bases para la **protección de datos personales**, incluyendo la **gestión de brechas de seguridad y la garantía de derechos digitales**.
- **Normas internacionales (ISO/IEC 27001 e ISO 22301):** Proporcionan un **marco de referencia reconocido internacionalmente** para la **gestión de la seguridad de la información y la continuidad del negocio**.

Este contrato tiene como finalidad **garantizar la correcta implementación y cumplimiento** de estos marcos normativos y estándares, promoviendo **homogeneidad, adaptabilidad y eficiencia** en las entidades locales, reforzando así su **capacidad de respuesta ante ciberamenazas** y asegurando una **protección uniforme en el ámbito regional**.

1.1.3 Rol estratégico de la Oficina de GRC

La Oficina de GRC de la Agencia desempeña un papel clave como **segunda línea de defensa** en el modelo de ciberseguridad regional. Su función principal es garantizar la **gestión eficaz del riesgo, el cumplimiento normativo y la gobernanza de la seguridad de la información**, proporcionando un soporte estructurado y estratégico a las entidades públicas de la Comunidad de Madrid.

Como parte de esta segunda línea de defensa, la Oficina de GRC **no sustituye las responsabilidades directas de la primera línea de defensa** dentro de cada entidad pública, sino que **facilita la implementación de marcos y políticas adecuados para la gestión de riesgos de ciberseguridad y el cumplimiento normativo**. En este contexto, contribuye de manera decisiva a la **resiliencia de los sistemas de información regionales** mediante las siguientes funciones clave:

- **Supervisión y alineación estratégica:** Garantizar que las políticas y procedimientos en materia de ciberseguridad implementados por las entidades públicas estén alineados con los objetivos estratégicos definidos por la Agencia.
- **Gestión proactiva del riesgo:** Proporcionar herramientas, metodologías y directrices para que las entidades identifiquen, analicen y mitiguen los riesgos asociados a sus activos críticos y

servicios esenciales, en **concordancia con el Esquema Nacional de Seguridad y otros marcos normativos aplicables**.

- **Desarrollo normativo y armonización de políticas:** Facilitar la creación, actualización y unificación de normativas internas, políticas y procedimientos de seguridad, **promoviendo la coherencia y homogeneidad entre las entidades locales**.
- **Asesoramiento técnico especializado:** Proveer orientación experta para la **implementación de controles, planes de actuación y medidas correctivas en materia de ciberseguridad y protección de datos**.

La Oficina de GRC es un pilar estratégico para la gestión eficaz de los riesgos de ciberseguridad en las entidades públicas, promoviendo la mejora continua y reforzando la gobernanza en un entorno normativo y tecnológico en constante evolución.

En coordinación con otras áreas clave de la Agencia, como la **Oficina de Auditoría** y el **CSIRT de la Comunidad de Madrid**, la Oficina de GRC garantiza la integración efectiva de políticas, metodologías y planes de acción en materia de gobierno, riesgo y cumplimiento. Esta colaboración asegura una alineación estratégica, permitiendo que los riesgos identificados, las oportunidades de mejora y las medidas preventivas se traduzcan en acciones operativas concretas, fortaleciendo así la postura de ciberseguridad a nivel regional.

1.1.4 Consolidación de la ciberseguridad en la Comunidad de Madrid

El presente contrato no solo busca reforzar la gobernanza, la gestión del riesgo y el cumplimiento normativo, sino también consolidar la ciberseguridad como un pilar estratégico para la sostenibilidad y resiliencia operativa de la Comunidad de Madrid. Para ello, la Oficina de GRC actúa como un facilitador estratégico, promoviendo las siguientes líneas de actuación:

- **Desarrollo de capacidades estructurales:** Proveer **herramientas, metodologías y directrices** que permitan a las entidades públicas gestionar eficazmente sus riesgos de ciberseguridad y alinearse con los estándares y normativas aplicables, garantizando su implementación de manera efectiva y sostenible.
- **Fortalecimiento de la gobernanza:** Impulsar una **toma de decisiones informada**, basada en el análisis y la priorización de riesgos, facilitando la **implementación de medidas preventivas y correctivas** que refuercen la confianza institucional y la protección de los servicios esenciales.
- **Homogeneización de buenas prácticas:** Fomentar la **coherencia en la implementación de normativas de ciberseguridad**, promoviendo políticas y procedimientos unificados que optimicen el uso de recursos y refuercen la seguridad a nivel regional.
- **Promoción de la mejora continua:** Impulsar una **cultura organizativa** basada en la evaluación y actualización constante de las prácticas de seguridad, asegurando la **adaptabilidad ante cambios** normativos, tecnológicos y en el panorama de amenazas.

Este enfoque garantiza que las entidades de la Administración pública de la Comunidad de Madrid, especialmente las entidades locales, cuenten con el soporte necesario para integrar la ciberseguridad en su modelo de gestión, consolidándola como un eje estratégico de gobernanza regional y fortaleciendo la protección de los servicios esenciales y los derechos de la ciudadanía.

1.2 Objetivos del contrato

El presente contrato tiene como **objetivo principal** reforzar la **capacidad operativa y técnica** de la **Oficina de Gobierno, Riesgo y Cumplimiento**, permitiéndole desempeñar su función como **facilitador estratégico** en la gestión del **riesgo, la gobernanza y el cumplimiento normativo** en materia de **ciberseguridad y protección de datos**. Se busca garantizar que las **entidades locales de la Comunidad de Madrid** implementen y mantengan **marcos normativos sólidos**, alineados con los estándares internacionales y adaptados a sus capacidades y recursos.

De manera específica, este contrato tiene los siguientes objetivos:

- **Implementación y mantenimiento de marcos normativos:** Apoyar a las entidades locales en la adecuación y aplicación de normativas de ciberseguridad y protección de datos, como el Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y el Reglamento General de Protección de Datos (RGPD), garantizando su cumplimiento efectivo.
- **Asistencia técnica en seguridad y cumplimiento:** Proporcionar apoyo especializado en la definición e implementación de controles, procedimientos internos y medidas organizativas, asegurando el cumplimiento normativo y la mitigación de riesgos.
- **Gestión integral de riesgos:** Identificar, analizar y priorizar amenazas de ciberseguridad, desarrollando planes de mitigación efectivos, basados en estándares internacionales como ISO/IEC 27001 e ISO 22301.
- **Mantenimiento y mejora continua del SGSI:** Asegurar la adaptación del Sistema de Gestión de Seguridad de la Información (SGSI) a los cambios normativos, tecnológicos y a la evolución de las ciberamenazas, optimizando su eficacia y sostenibilidad.
- **Desarrollo de normativas internas y procedimientos:** Facilitar la creación y actualización de normas, políticas y procedimientos de seguridad, promoviendo la coherencia y homogeneidad en su aplicación en las entidades locales.
- **Evaluaciones periódicas y mejora continua:** Realizar revisiones sistemáticas del cumplimiento normativo, proporcionando informes técnicos que orienten la toma de decisiones y fomenten el avance progresivo en ciberseguridad.
- **Formación y sensibilización:** Diseñar e impartir programas de capacitación para responsables de ciberseguridad y personal técnico, promoviendo una cultura organizativa que priorice la ciberseguridad como un eje estratégico en la gestión pública.

CLÁUSULA 2.- OBJETO Y ALCANCE DEL CONTRATO

2.1 Descripción general de los servicios requeridos

El presente contrato tiene como **objetivo principal** la prestación de **servicios especializados** para **fortalecer la capacidad operativa y técnica** de la **Oficina de GRC** de la Agencia de Ciberseguridad. Estos servicios están dirigidos a **garantizar la implementación, seguimiento y mejora continua** de las **normativas y estándares de ciberseguridad y protección de datos** en las entidades locales de la Comunidad de Madrid, con especial prioridad en aquellas de **menos de 20.000 habitantes**, que enfrentan mayores **limitaciones de recursos**.

A través de este contrato, se busca:

- Facilitar la **adopción y cumplimiento de marcos normativos** de ciberseguridad en las entidades locales.
- Promover la **gestión proactiva de riesgos** y la mejora continua de la seguridad de la información.
- Desarrollar **políticas, normas y procedimientos estandarizados** que garanticen una ciberseguridad resiliente y sostenible, alineada con los objetivos estratégicos de la Agencia y los requisitos legales aplicables.

Los servicios se adaptarán a las **necesidades específicas de cada entidad local**, considerando su **nivel de madurez tecnológica, recursos disponibles y grado de exposición a riesgos de ciberseguridad**.

Además, el enfoque del contrato está diseñado para fomentar la **sostenibilidad operativa a largo plazo**, dotando a las entidades locales de las **herramientas, conocimientos y capacidades necesarias** para gestionar la ciberseguridad de forma autónoma. Para evaluar el impacto de los

servicios, se establecerán **indicadores clave de rendimiento**, asegurando la **mejora continua y alineación con los objetivos estratégicos de la Agencia**.

Las áreas clave de actuación incluidas en el alcance del contrato son las siguientes:

1. Cumplimiento normativo en ciberseguridad y protección de datos:

- Asistencia técnica para la implementación y adecuación al Esquema Nacional de Seguridad (ENS), la Directiva NIS2, el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Supervisión del nivel de cumplimiento normativo y propuesta de medidas correctivas para subsanar desviaciones.

2. Gestión de riesgos de ciberseguridad:

- Identificación, análisis y priorización de riesgos que comprometan los servicios esenciales y activos críticos de las entidades locales.
- Diseño y propuesta de planes de mitigación y medidas correctivas, alineados con estándares internacionales como ISO/IEC 27001 e ISO 22301, adaptados al contexto de cada entidad.

3. Soporte al Sistema de Gestión de Seguridad de la Información (SGSI):

- Apoyo en la implementación, operación y mejora continua de los SGSI, garantizando su actualización frente a cambios normativos, tecnológicos y en el entorno de amenazas.
- Fomento de la alineación del SGSI con el ENS y las mejores prácticas internacionales.

4. Desarrollo de normativas y políticas internas:

- Asesoramiento técnico en la redacción y actualización de normativas internas, políticas y procedimientos, promoviendo la coherencia y homogeneidad en la gestión de la seguridad de la información entre las entidades locales.

5. Formación y sensibilización en GRC:

- Diseño e impartición de programas de capacitación para responsables de ciberseguridad, personal técnico y cargos electos, enfocados en fortalecer sus competencias en la gestión del riesgo y el cumplimiento normativo.
- Promoción de una cultura de ciberseguridad proactiva dentro de las organizaciones.

6. Seguimiento y reporte:

- Elaboración de informes técnicos y reportes periódicos que evalúen el nivel de madurez en ciberseguridad y sugieran medidas concretas para su mejora.

7. Coordinación con otras áreas clave de la Agencia:

- Colaboración con áreas clave de la Agencia, como la Oficina de Auditoría y el CSIRT de la Comunidad de Madrid, para garantizar una integración efectiva de las actividades de GRC dentro del marco estratégico de ciberseguridad regional.

2.2 Ámbito de aplicación y alcance funcional

El presente contrato se aplica a las **entidades locales de la Comunidad de Madrid**, en el marco de las competencias definidas en la **Ley 14/2023**, por la que se creó la **Agencia de Ciberseguridad de la Comunidad de Madrid**. Su enfoque se centra en **fortalecer la gobernanza, la gestión de riesgos y el cumplimiento normativo** en dichas entidades, con especial atención a aquellas con **menos de 20.000 habitantes**, que presentan mayores **limitaciones de recursos técnicos y organizativos** para garantizar su ciberseguridad.

El **alcance funcional** del contrato abarca los **servicios descritos en el apartado 2.1**, estructurados dentro de un **programa anual de implantación de marcos normativos**, aprobado por la Agencia

de Ciberseguridad y gestionado por su Oficina de GRC. Este programa define las **prioridades, actividades y recursos** a asignar en función de los siguientes criterios:

- **Nivel de riesgo** de las entidades locales.
- **Impacto potencial** en la resiliencia de los servicios esenciales.
- **Necesidades estratégicas** identificadas por la Agencia de Ciberseguridad.

Es importante señalar que **no todas las entidades locales** incluidas en el **ámbito de aplicación** serán objeto de **todas las actividades** descritas en este contrato. **El programa anual definirá las prioridades y los recursos asignados**, en función de los mismos criterios indicados anteriormente.

CLÁUSULA 3.- REQUISITOS GENERALES

3.1 Requisitos básicos

El adjudicatario deberá cumplir con una serie de **requisitos fundamentales** para garantizar que los servicios prestados sean de **alta calidad, eficaces y alineados** con los objetivos estratégicos de la Agencia. Estos requisitos se estructuran en tres áreas principales: **técnicos, operativos y de comunicación y soporte**.

3.1.1 Requisitos técnicos

- **Cumplimiento normativo y alineación con estándares internacionales:** Los servicios deben cumplir con las normativas aplicables en ciberseguridad y protección de datos, incluyendo el **Esquema Nacional de Seguridad, la Directiva NIS2 (Directiva (UE) 2022/2555), el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)**. Asimismo, deberán alinearse con estándares internacionales como **ISO/IEC 27001 e ISO 22301**, asegurando las **mejores prácticas en seguridad de la información y continuidad de negocio**.
- **Garantías de confidencialidad y seguridad de la información:** El adjudicatario deberá **implementar controles estrictos** para proteger toda la información manejada durante la ejecución del contrato, garantizando su **integridad, disponibilidad y confidencialidad**. Además, deberá notificar **de inmediato** cualquier incidente de seguridad, gestionándolo conforme a los **protocolos establecidos por la Agencia**.
- **Uso de herramientas especializadas:** Se deberán emplear herramientas actualizadas y **compatibles** con los sistemas de la Agencia y las entidades locales para la **implantación de marcos normativos, la gestión de riesgos y la elaboración de informes**. Estas herramientas deberán ser **verificadas** y cumplir con los requisitos técnicos establecidos.

3.1.2 Requisitos operativos y de gestión

- **Cumplimiento de plazos y cronogramas:** Todas las actividades deberán ejecutarse **dentro de los plazos estipulados en el contrato**. En caso de **desviaciones**, estas deberán **justificarse** y acompañarse de **medidas correctivas aprobadas** por la Agencia.
- **Adaptación a las necesidades de las entidades locales:** Los servicios deberán ajustarse a las **características específicas de cada entidad local**, considerando su **nivel de madurez, tamaño y recursos disponibles**. Esto garantizará que las soluciones sean **efectivas, viables y escalables**.
- **Control interno de calidad:** El adjudicatario deberá **implementar un sistema de control de calidad** que supervise la ejecución de los servicios, identifique **desviaciones** y aplique **medidas correctivas** para asegurar el cumplimiento de los objetivos del contrato.

3.1.3 Requisitos de comunicación y soporte

- **Colaboración con la Agencia y otras áreas técnicas:** El adjudicatario deberá **coordinarse estrechamente** con las áreas clave de la Agencia, incluyendo el **CSIRT de la Comunidad de Madrid y la Oficina de Auditoría**, asegurando la **integración efectiva** de los servicios en los procesos estratégicos.
- **Disponibilidad de recursos:** Se deberá garantizar la **disponibilidad de los recursos humanos y técnicos necesarios** para cumplir con las exigencias del contrato, **ajustándose a las necesidades justificadas por la Agencia**.
- **Propuesta de mejora continua:** Al término del contrato, el adjudicatario deberá presentar un **informe final con recomendaciones prácticas y estratégicas**, orientadas a **optimizar los procesos implementados y fortalecer la ciberseguridad** en las entidades locales.

3.2 Cumplimiento de normativa específica

El adjudicatario será responsable de garantizar que los **servicios prestados**, y los productos obtenidos como consecuencia de esta prestación, cumplan con la **normativa vigente** en materia de ciberseguridad y seguridad de la información. Asimismo, deberá **aplicar las guías y recomendaciones técnicas** emitidas por organismos competentes, en particular aquellas relacionadas con el **Esquema Nacional de Seguridad y la Directiva NIS2 (Directiva (UE) 2022/2555)**, incluyendo su transposición al marco normativo español.

3.2.1 Normativa aplicable

En **complemento** al marco normativo mencionado en el apartado **1.1.2**, el adjudicatario deberá:

- **Aplicar de forma operativa los principios y medidas del ENS y la Directiva NIS2:** Todas las actividades deberán garantizar el cumplimiento de los **controles mínimos y específicos establecidos en el ENS (Real Decreto 311/2022) y en la Directiva NIS2**, su transposición y normas derivadas o complementarias. Esto incluye la implementación de medidas **organizativas y técnicas exigidas** para la seguridad de los sistemas y servicios esenciales.
- **Integrar los requisitos de protección de datos personales:** Asegurar que las entidades locales **implementen medidas técnicas y organizativas adecuadas** para el cumplimiento del **RGPD y la LOPDGDD**, particularmente en aspectos como la **gestión de brechas de seguridad**, la **protección de los derechos de los interesados y la privacidad en la prestación de servicios**.
- **Adaptarse a la evolución del marco normativo:** Supervisar cualquier **modificación o actualización** de las normativas relevantes durante la vigencia del contrato, incluyendo aquellas derivadas de la **transposición de la Directiva NIS2 a través del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad** y de las futuras normativas sectoriales complementarias. El adjudicatario deberá **reflejar estos cambios** en sus actividades y procedimientos de manera ágil y efectiva.

3.2.2 Recomendaciones técnicas

El adjudicatario deberá **basar su actuación** en las guías técnicas publicadas por el **Centro Criptológico Nacional (CCN)**, en especial aquellas aplicables al **Esquema Nacional de Seguridad (ENS)**. Entre ellas:

- **Guías de auditoría y verificación del ENS:** Se deberán seguir las **pautas para la implementación y seguimiento de controles de seguridad exigidos**, asegurando la **conformidad de las entidades locales** con los requisitos normativos.
- **Perfiles de cumplimiento y medidas específicas:** Aplicación de las recomendaciones contenidas en las **guías CCN-STIC**, adaptando los controles y medidas a la **naturaleza de cada entidad local**.

El adjudicatario deberá garantizar que las **metodologías y herramientas utilizadas** estén actualizadas según las guías técnicas más recientes del **CCN-STIC**.

3.2.3 Controles específicos del proceso de adecuación normativa

El adjudicatario deberá aplicar **controles específicos** para evaluar y fortalecer la **gobernanza, la gestión de riesgos y el cumplimiento normativo** en las entidades locales. Estos controles incluyen:

- **Medidas de seguridad derivadas del ENS, NIS2 y RGPD:** Verificar la **existencia, eficacia e implementación** de los **controles y procedimientos técnicos y organizativos** exigidos en estas normativas.
- **Gestión integral de riesgos en ciberseguridad:** Evaluar los procesos utilizados por las entidades para **identificar, analizar, priorizar y mitigar riesgos**, asegurando su alineación con **estándares internacionales como ISO/IEC 27001 e ISO 22301**.
- **Planes de continuidad y resiliencia:** Revisar la existencia y adecuación de los **planes de continuidad operativa y recuperación ante desastres**, asegurando que sean **efectivos** y garanticen la **resiliencia de los servicios esenciales**.
- **Capacidades de detección, respuesta y notificación de incidentes:** Analizar si las entidades cuentan con los **mecanismos adecuados** para **detectar, gestionar y notificar incidentes de seguridad**, conforme a los requerimientos del **ENS, la Directiva NIS2 y su transposición**.

El adjudicatario deberá adoptar un **enfoque integral y flexible**, permitiendo la **personalización de los controles y actividades** según las **características y necesidades específicas de cada entidad local**. Asimismo, deberá asegurar que las **medidas implementadas sean sostenibles** y estén alineadas con las **mejores prácticas internacionales y normativas vigentes**.

CLÁUSULA 4.- CAPACIDADES, FUNCIONES Y SERVICIOS A PRESTAR

4.1 Capacidades clave de la Oficina de GRC

La Oficina de GRC desempeña un papel estratégico en el modelo de ciberseguridad de la Comunidad de Madrid, actuando como la **segunda línea de defensa** para garantizar la **gobernanza, la gestión de riesgos y el cumplimiento normativo** en las entidades locales.

Sus capacidades se organizan en torno a **tres áreas esenciales**:

- **Implementación y cumplimiento normativo:** Proporcionar directrices, herramientas y soporte técnico para ayudar a las entidades locales a cumplir con los marcos regulatorios aplicables.
- **Gestión integral de riesgos:** Definir metodologías prácticas para la identificación, análisis y priorización de riesgos en ciberseguridad, promoviendo un enfoque preventivo y proactivo en su gestión.
- **Fomento de la mejora continua:** Aplicar un enfoque basado en evidencia para el fortalecimiento de la ciberseguridad en las entidades locales, optimizando recursos y garantizando la sostenibilidad de las medidas implementadas.

La Oficina de GRC actúa como un **facilitador estratégico**, proporcionando un **marco integral de apoyo** para la **adopción de normativas, la mitigación de riesgos y la consolidación de una cultura organizativa centrada en la ciberseguridad**.

4.1.1 Implementación y cumplimiento normativo

La **Oficina de GRC** será responsable de:

- **Apoyar la implementación de marcos normativos aplicables:** Facilitar la adecuación de las entidades locales a las normativas, asegurando la adopción de medidas técnicas y organizativas para garantizar la conformidad normativa.
- **Supervisar y evaluar el grado de cumplimiento:** Proporcionar herramientas y procedimientos que permitan a las entidades locales verificar su grado de cumplimiento normativo, identificar desviaciones y proponer acciones correctivas.

4.1.2 Gestión integral de riesgos

La Oficina de GRC será un referente clave en la **gestión de riesgos de ciberseguridad** en las entidades locales, asegurando:

- **Identificación y priorización de riesgos:** Implementar procesos estructurados para la identificación de activos críticos, evaluación de amenazas y vulnerabilidades, y priorización de riesgos en función de su impacto y probabilidad.
- **Desarrollo de planes de mitigación:** Establecer directrices claras para el diseño y ejecución de planes de acción que reduzcan los riesgos identificados, alineándolos con estándares internacionales como ISO/IEC 27001 e ISO 22301.
- **Seguimiento de la efectividad de las medidas:** Revisar la implementación de las acciones correctivas y evaluar su eficacia en el tiempo, promoviendo una cultura de mejora continua en la ciberseguridad de las entidades locales.

4.1.3 Desarrollo de capacidades y mejora continua

La Oficina de GRC no solo se centra en la **implementación y evaluación de normativas**, sino también en la **generación de capacidades sostenibles** en las entidades locales.

- **Capacitación y sensibilización:** Diseñar e impartir programas de formación específicos del ámbito de GRC, dirigidos a responsables de ciberseguridad, personal técnico y cargos electos, fomentando una cultura organizativa enfocada en la ciberseguridad.
- **Supervisión de planes de mejora:** Acompañar a las entidades locales en el diseño, ejecución y monitoreo de planes de mejora, basados en hallazgos y análisis de riesgos, garantizando que las soluciones implementadas sean sostenibles y efectivas.
- **Optimización de recursos:** Promover la eficiencia en el uso de recursos, a través de la estandarización de procesos y la priorización estratégica de actividades, maximizando el impacto de las acciones implementadas.

4.2 Servicios detallados por ámbito

La Oficina de GRC desarrollará su labor mediante una serie de **servicios especializados**, estructurados en torno a los **ámbitos clave de actuación** definidos en los apartados 2.1 (Descripción general de los servicios requeridos) y 3.1 (Requisitos básicos).

Estos servicios tienen como objetivo **consolidar la gobernanza, fortalecer la gestión de riesgos y garantizar el cumplimiento normativo** en las entidades locales de la Comunidad de Madrid.

A continuación, se presenta una **síntesis de los servicios detallados**, destacando elementos adicionales que complementan las capacidades descritas previamente:

4.2.1 Apoyo en la implementación de marcos normativos

Este servicio, descrito en el apartado 2.1, se centrará en:

- **Proveer herramientas prácticas y asistencia técnica** que permitan a las entidades locales adecuarse al Esquema Nacional de Seguridad, la Directiva NIS2 y las normativas de protección de datos.

- **Diseñar hojas de ruta específicas** para cada entidad local, asegurando que las actividades de implementación se ajusten a sus recursos y necesidades, optimizando el uso de las capacidades disponibles.

4.2.2 Gestión integral de riesgos

En línea con lo indicado en los apartados **2.1** y **3.1**, este servicio incluye:

- **Realizar análisis de riesgos personalizados** para identificar activos críticos y amenazas específicas que afecten a los servicios esenciales de las entidades locales.
- **Priorizar los riesgos** según su impacto y probabilidad, proporcionando planes de acción concretos y accesibles para su mitigación, basados en estándares como ISO/IEC 27001 e ISO 22301.
- **Asegurar que las recomendaciones emitidas** sean prácticas, medibles y adaptadas al contexto de cada entidad.

4.2.3 Supervisión de controles técnicos y organizativos

En línea con lo indicado en los apartados **2.1** y **3.1**, la Oficina supervisará la efectividad y adecuación de los controles implementados, aportando los siguientes detalles adicionales:

- **Controles técnicos:** Verificación del diseño e implementación de medidas existentes, asegurando su alineación con las guías del CCN-STIC y otras mejores prácticas reconocidas.
- **Controles organizativos:** Evaluación de políticas internas y procedimientos existentes relacionados con la ciberseguridad, verificando su claridad, aplicabilidad y comunicación efectiva dentro de la organización.

4.2.4 Formación y sensibilización

Como se detalla en el apartado **2.1**, este servicio busca fortalecer las capacidades internas de las entidades locales. Esto se deberá realizar mediante:

- **Programas de formación** adaptados a distintos niveles de responsabilidad, desde altos cargos hasta personal técnico.
- **Talleres prácticos** enfocados en la gestión de incidentes, mitigación de riesgos y mejora de los controles existentes.
- **Desarrollo de materiales formativos** personalizados que sirvan como referencia a largo plazo.

4.2.5 Generación de informes y recomendaciones

Este servicio, complementario al apartado **3.2**, incluye:

- **Elaboración de informes técnicos** estructurados que detallen el grado de implantación de los controles más relevantes, incluyendo un resumen ejecutivo accesible para la alta dirección.
- **Propuestas de mejora priorizadas**, acompañadas de indicadores clave de rendimiento (KPI) que permitan monitorizar el progreso y evaluar el impacto de las acciones correctivas.

4.2.6 Alineación estratégica con la Agencia

Como se menciona en los apartados **2.1** y **3.1.3**, todos los servicios estarán alineados con los objetivos estratégicos de la Agencia de Ciberseguridad. Además:

- Se establecerán reuniones periódicas con otras áreas clave de la Agencia, como la Oficina de Auditoría y el CSIRT, para **asegurar la integración efectiva de las actividades de GRC** en el marco estratégico regional.

- Los resultados obtenidos se comunicarán de forma estructurada para **fomentar la toma de decisiones** basada en datos.

CLÁUSULA 5.- EQUIPO DE TRABAJO

5.1 Perfiles requeridos

El adjudicatario deberá garantizar que el equipo asignado al contrato cuente con profesionales altamente cualificados, cuya experiencia y competencias se ajusten a los requerimientos establecidos en este pliego. La correcta configuración del equipo de trabajo será un factor crítico para el éxito del contrato y el cumplimiento de los objetivos estratégicos de la Agencia.

El equipo deberá estar compuesto por los perfiles detallados a continuación, asegurando la dedicación establecida para cada uno. Cualquier incumplimiento en la provisión de los perfiles exigidos podrá constituir causa de resolución del contrato.

5.1.1 Perfiles y responsabilidades clave

- **Responsable de Servicio (1 puesto, 50% de dedicación)**

Este profesional tendrá la responsabilidad de liderar el equipo de trabajo, asegurando la correcta planificación, ejecución y supervisión de las actividades encomendadas a la Oficina de GRC. Sus funciones deberán ser:

- Coordinar la ejecución del contrato y supervisar el cumplimiento de los objetivos estratégicos establecidos.
- Actuar como punto de contacto principal con la Agencia de Ciberseguridad, asegurando una comunicación fluida y un reporte adecuado del estado de los trabajos.
- Gestionar la planificación de tareas y la distribución del equipo de trabajo, asegurando la correcta asignación de recursos y la optimización de esfuerzos.
- Garantizar la calidad y consistencia de los entregables generados, supervisando su alineación con los marcos normativos aplicables.

- **Arquitecto de Seguridad (1 puesto, 100% de dedicación)**

Este profesional será responsable de definir la arquitectura de seguridad y los controles técnicos necesarios para la correcta implementación de los marcos normativos y estándares de seguridad aplicables. Sus funciones deberán ser:

- Diseñar e implementar estrategias de seguridad alineadas con los requisitos del ENS, la Directiva NIS2 y los estándares internacionales.
- Evaluar la adecuación y eficacia de los controles técnicos implementados en las entidades locales, proponiendo mejoras basadas en las mejores prácticas del sector.
- Asegurar la integración de soluciones de seguridad en los procesos y sistemas de las entidades, facilitando su cumplimiento normativo.

- **Consultor Senior GRC - Especialista Técnico (1 puesto, 100% de dedicación)**

Este perfil tendrá un papel clave en la supervisión técnica y operativa de la gestión de riesgos en ciberseguridad dentro de las entidades locales. Las responsabilidades deberán ser:

- Identificar, analizar y gestionar riesgos tecnológicos en los sistemas de información de las entidades locales.
- Definir controles y medidas de mitigación basadas en estándares como ISO/IEC 27001 e ISO 22301, asegurando su correcta aplicación.
- Evaluar la implementación y efectividad de los marcos normativos de ciberseguridad en las entidades locales, proponiendo mejoras.

- **Consultor Mid Senior GRC - Ámbito Compliance Legal (1 puesto, 100% de dedicación)**

Este perfil aporta la especialización en garantizar el alineamiento normativo de las entidades locales con los requisitos legales y regulatorios aplicables en materia de ciberseguridad y protección de datos, con las siguientes funciones principales:

- Analizar la adecuación de las entidades locales al ENS, la Directiva NIS2 y la normativa de protección de datos (RGPD, LOPDGDD).
- Asesorar en la definición e implementación de políticas de cumplimiento, asegurando su coherencia con los requisitos regulatorios.
- Elaborar informes de cumplimiento y propuestas de mejora que permitan optimizar la postura de seguridad de las entidades locales.

- **Analista de Seguridad (1 puesto, 100% de dedicación)**

Este profesional será responsable del análisis, seguimiento y documentación de los procesos de seguridad implementados en las entidades locales, desempeñando las siguientes funciones:

- Monitorear y evaluar la ejecución de controles de seguridad en las entidades locales, identificando áreas de mejora.
- Apoyar en la recopilación de evidencias y en la documentación de hallazgos, asegurando su correcta gestión.
- Colaborar en la elaboración de informes técnicos, proporcionando información clave para la toma de decisiones en materia de ciberseguridad.

5.2 Requisitos de formación y experiencia

A continuación, se detallan los requisitos mínimos de formación y experiencia para los perfiles solicitados:

5.2.1 Responsable de Servicio

- **Formación:** Título universitario MECES 2 o superior en áreas relacionadas con la ciberseguridad, tecnologías de la información, ingeniería o disciplinas afines.
- **Certificaciones:** Al menos dos (2) certificaciones vigentes entre las siguientes:
 - **ISACA CISA** (Certified Information Systems Auditor)
 - **ISACA CISM** (Certified Information Security Manager)
 - **ISACA CRISC** (Certified In Risk And Information Systems Control)
 - **(ISC)² CISSP** (Certified Information Systems Security Professional)
 - **EC-Council C|CISO** (Certified Chief Information Security Officer)
 - **EC-Council CEH** (Certified Ethical Hacker)
 - **ISMS FORUM CPCC** (Certified Professional Cyber Compliance)
 - **ISMS FORUM CCSP** (Certified Cyber Security Professional)
 - **ISO 22301 Internal / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - **ISO 27001 Internal / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - **PMI PMP** (Project Management Professional)
 - **PRINCE2 Practitioner** (PRjects IN Controlled Environments)
 - **IPMA Nivel C o superior** (International Project Management Association)
 - **PM2 Nivel 2 o superior** (Project Management Methodology de la Comisión Europea)

- **ITIL v4 Managing Professional o superior** (Axelos)
- **ISO 20000 Internal / Lead Auditor** (Acreditado por Entidad de Certificación)
- Además, se considerará como una certificación válida la posesión de un **máster universitario** relacionado con el ámbito de la ciberseguridad, gestión de servicios de TI, o gestión de proyectos, o la finalización de un programa académico con una duración mínima de **1.500 horas de trabajo**, siempre que esté relacionado con estas áreas y avalado por una institución reconocida.
- **Experiencia:**
 - Al menos 6 años de experiencia en consultoría de ciberseguridad o gestión de riesgos tecnológicos, de los cuales al menos 3 años deben haber sido en roles de liderazgo de equipos multidisciplinares.
 - Experiencia en la planificación y supervisión de procesos de adecuación normativa, con normativas como el ENS, la Directiva NIS/NIS2 y estándares internacionales (ISO 27001, ISO 22301).
 - Conocimiento avanzado en metodologías de análisis de riesgos, tales como MAGERIT, y experiencia en la elaboración de planes de tratamiento de riesgos o de mejora de la seguridad.

5.2.2 Arquitecto de Seguridad

- **Formación:** Título universitario MECES 2 o superior en Ingeniería Informática, Telecomunicaciones, Tecnologías de la Información o áreas técnicas relacionadas con la ciberseguridad.
- **Certificaciones:** Al menos dos (2) certificaciones vigentes entre las siguientes:
 - **ISACA CISA** (Certified Information Systems Auditor)
 - **ISACA CRISC** (Certified In Risk And Information Systems Control)
 - **(ISC)² CISSP** (Certified Information Systems Security Professional)
 - **(ISC)² CCSP** (Certified Cloud Security Professional)
 - **OSCP** (Offensive Security Certified Professional)
 - **EC-Council CEH** (Certified Ethical Hacker)
 - **EC-Council CHFI** (Computer Hacking Forensics Investigator)
 - **CompTIA Security+**
 - **ISACA CSX** (Cybersecurity Fundamentals Certificate)
 - **AWS Cloud Practitioner**
 - **GSEC** (SANS GIAC Security Essentials)
 - **ISMS FORUM CCSP** (Certified Cyber Security Professional)
 - **Cisco CCNP** (Certified Network Professional Security)
 - **ISO 22301 Internal / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - **ISO 27001 Internal / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - Además, se considerará como una certificación válida la posesión de un **máster universitario** relacionado con el ámbito de la ciberseguridad, o la finalización de un programa académico con una duración mínima de **1.500 horas de trabajo**, siempre que esté relacionado con la ciberseguridad o la seguridad de la información y avalado por una institución reconocida.

- **Experiencia:**

- Al menos 3 años de experiencia en seguridad de la información y ciberseguridad, con un enfoque en la definición, implementación y supervisión de arquitecturas de seguridad en entornos tecnológicos complejos.
- Experiencia demostrable en el diseño y despliegue de controles técnicos de seguridad, incluyendo segmentación de redes, autenticación multifactor, gestión de accesos privilegiados y protección de la información.
- Conocimiento profundo en frameworks y normativas de seguridad, incluyendo ENS, Directiva NIS2, ISO/IEC 27001, ISO/IEC 27005 y guías CCN-STIC, con capacidad para traducir sus requisitos en medidas técnicas concretas.

5.2.3 Consultor Senior GRC - Especialista Técnico

- **Formación:** Título universitario MECES 2 o superior en Ingeniería Informática, Telecomunicaciones, Tecnologías de la Información o áreas técnicas relacionadas con la ciberseguridad.
- **Certificaciones:** Al menos dos (2) certificaciones vigentes entre las siguientes:
 - **ISACA CISA** (Certified Information Systems Auditor)
 - **ISACA CRISC** (Certified In Risk And Information Systems Control)
 - **(ISC)² CISSP** (Certified Information Systems Security Professional)
 - **(ISC)² CCSP** (Certified Cloud Security Professional)
 - **OSCP** (Offensive Security Certified Professional)
 - **EC-Council CEH** (Certified Ethical Hacker)
 - **EC-Council CHFI** (Computer Hacking Forensics Investigator)
 - **CompTIA Security+**
 - **ISACA CSX** (Cybersecurity Fundamentals Certificate)
 - **GSEC** (SANS GIAC Security Essentials)
 - **ISMS FORUM CCSP** (Certified Cyber Security Professional)
 - **Cisco CCNP** (Certified Network Professional Security)
 - **ISO 22301 Internal / Lead Auditor** (Acreditado por Entidad de Certificación)
 - **ISO 27001 Internal / Lead Auditor** (Acreditado por Entidad de Certificación)
- Además, se considerará como una certificación válida la posesión de un **máster universitario** relacionado con el ámbito de la ciberseguridad, o la finalización de un programa académico con una duración mínima de **1.500 horas de trabajo**, siempre que esté relacionado con la ciberseguridad o la seguridad de la información y avalado por una institución reconocida.
- **Experiencia:**
 - Al menos 4 años de experiencia profesional en revisiones técnicas de la seguridad en sistemas de información, y controles de ciberseguridad en entornos tecnológicos complejos.
 - Experiencia en el análisis de configuraciones de seguridad, segmentación de redes, gestión de accesos y aplicaciones de herramientas como MAGERIT y PILAR.
 - Habilidades avanzadas para identificar vulnerabilidades técnicas y proponer soluciones innovadoras y prácticas.

5.2.4 *Consultor Mid Senior GRC - Ámbito Compliance Legal*

- **Formación:** Título universitario MECES 2 o superior en Derecho, Ciencias Jurídicas o áreas relacionadas, con especialización en ciberseguridad, protección de datos o cumplimiento normativo.
- **Certificaciones:** Al menos dos (2) certificaciones vigentes entre las siguientes:
 - **ISACA CISA** (Certified Information Systems Auditor)
 - **ISACA CISM** (Certified Information Security Manager)
 - **ISACA CDPSE** (Certified Data Privacy Solutions Engineer)
 - **ISACA CRISC** (Certified In Risk And Information Systems Control)
 - **ISMS FORUM CPCC** (Certified Professional Cyber Compliance)
 - **ISACA CSX** (Cybersecurity Fundamentals Certificate)
 - **(ISC)² CC** (Certified in Cybersecurity)
 - **(ISC)² CISSP** (Certified Information Systems Security Professional)
 - **(ISC)² CCSP** (Certified Cloud Security Professional)
 - **ISO 22301 Lead / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - **ISO 27001 Lead / Lead Auditor o Implementer** (Acreditado por Entidad de Certificación)
 - **ISO 27701 Lead Auditor / Implementer** (Acreditado por Entidad de Certificación)
 - **Delegado de Protección de Datos**, reconocido por la Agencia Española de Protección de Datos
 - **IAPP CIPP/E** (Certified Information Privacy Professional/Europe)
 - Además, se considerará como una certificación válida la posesión de un **máster universitario** relacionado con el ámbito de la ciberseguridad, o la finalización de un programa académico con una duración mínima de **1.500 horas de trabajo**, siempre que esté relacionado con la ciberseguridad, la seguridad de la información, la privacidad o el cumplimiento normativo TI, y avalado por una institución reconocida.
- **Experiencia:**
 - Al menos 2 años de experiencia profesional consultoría o auditoría de ámbito cumplimiento normativo en seguridad de la información y ciberseguridad.
 - Experiencia en la evaluación de políticas internas y normativas relacionadas con la ciberseguridad y la protección de datos.
 - Capacidad para identificar brechas legales y proponer medidas correctivas prácticas y alineadas con las normativas aplicables.

5.2.5 *Analista de Seguridad*

- **Formación:** Título universitario MECES 2 o superior en áreas técnicas relacionadas con ciberseguridad, tecnologías de la información o auditoría.
- **Certificaciones:** No se requieren certificaciones específicas.
- **Experiencia:**
 - Al menos 1 año de experiencia en proyectos relacionados con ciberseguridad.
 - Conocimiento básico de herramientas de análisis de riesgos, gobernanza de la seguridad de la información y ciberseguridad, y auditoría, así como de normativas como el ENS o el RGPD.

5.2.6 Requisitos generales adicionales para todo el equipo

Además de los requisitos específicos detallados para cada perfil, el equipo de trabajo en su conjunto deberá cumplir con una serie de competencias generales que garanticen la excelencia en la ejecución de las actividades de auditoría. Estas competencias, basadas en el conocimiento actualizado de normativas, el dominio de herramientas especializadas y la experiencia en entornos públicos, son fundamentales para asegurar la calidad y efectividad de los servicios prestados. Los siguientes requisitos serán de aplicación a todos los integrantes del equipo:

- **Conocimiento normativo actualizado:** Todos los miembros deberán demostrar un entendimiento práctico y vigente de las normativas aplicables al ámbito de la ciberseguridad y la protección de datos, tales como el Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y el Reglamento General de Protección de Datos (RGPD). También se valorará el conocimiento en la Ley Orgánica 3/2018 (LOPDGDD) y su integración con las normativas mencionadas.
- **Dominio de guías técnicas:** Se exigirá familiaridad con las guías técnicas emitidas por el Centro Criptológico Nacional (CCN-STIC), en particular aquellas relacionadas con auditorías, análisis de riesgos y perfiles de cumplimiento, como CCN-STIC 802, 808, 890A, 890C y 892. El equipo deberá demostrar capacidad para implementar las normas o mejores prácticas recomendadas de estas guías.
- **Competencia en herramientas especializadas:** Todos los integrantes deberán estar capacitados para utilizar herramientas de auditoría y análisis de riesgos reconocidas en el sector, tales como MAGERIT, PILAR y CLARA. Además, deberán poder integrarlas eficazmente en los procesos de evaluación y generación de informes.
- **Experiencia en el sector público:** Se valorará positivamente la experiencia previa en auditorías de ciberseguridad realizadas en entidades públicas o en entornos regulados, lo que permitirá una mejor adaptación a los procedimientos y particularidades del ámbito de actuación de la Agencia.
- **Compromiso con la mejora continua:** El equipo deberá estar dispuesto a participar en procesos de formación continua y actualización, con el objetivo de garantizar la adaptación a posibles cambios normativos y tecnológicos durante la vigencia del contrato.

5.3 Cambios en el equipo a solicitud de la Agencia

La Agencia se reserva el derecho de solicitar cambios en el equipo de trabajo asignado por el adjudicatario cuando concurren circunstancias que puedan comprometer la calidad, eficacia o alineación estratégica de los servicios prestados. Esta facultad tiene como objetivo garantizar que el equipo cumpla con los requisitos establecidos en el contrato y mantenga los niveles de excelencia exigidos.

5.3.1 Supuestos para solicitar cambios en el equipo

A continuación, se describen las situaciones específicas que justificarán solicitudes de cambio:

- **Deficiencia en el desempeño:** Cuando se identifiquen insuficiencias reiteradas en la ejecución de las tareas asignadas, incumplimientos de plazos o estándares de calidad, y dichas deficiencias no hayan sido subsanadas tras la correspondiente notificación y período de corrección.
- **Falta de cualificación o experiencia:** Si se detecta que alguno de los miembros del equipo no cumple con los requisitos de formación, certificaciones o experiencia especificados en este pliego, o si su desempeño demuestra carencias técnicas o de conocimiento.
- **Incompatibilidad o conflictos:** En casos de incompatibilidad manifiesta con los procedimientos internos de la Agencia, falta de colaboración efectiva o conflictos con otros miembros del equipo o con el personal de la Agencia.

- **Rotación por necesidades del adjudicatario:** Si el adjudicatario propone cambios en el equipo por motivos internos, la Agencia evaluará previamente las propuestas y podrá solicitar ajustes o rechazar la modificación si considera que afecta negativamente a la prestación del servicio.

5.3.2 Procedimiento para solicitar cambios en el equipo

La solicitud de cambios en el equipo asignado al contrato seguirá un procedimiento claro y estructurado que garantice la transparencia, la efectividad de la transición y la continuidad del servicio. Este proceso, diseñado para minimizar impactos negativos, busca asegurar que las modificaciones en el equipo se realicen de forma ordenada y con el debido respaldo documental. A continuación, se detallan los pasos específicos que conforman dicho procedimiento:

- **Notificación formal de la Agencia:** La Agencia comunicará por escrito al adjudicatario la necesidad de realizar cambios en el equipo, indicando las razones específicas y proporcionando evidencias que justifiquen la solicitud.
- **Propuesta del adjudicatario:** El adjudicatario tendrá un plazo máximo de **15 días hábiles** para presentar un plan de sustitución que incluya los perfiles propuestos, sus certificaciones y experiencia relevante.
- **Evaluación y aprobación de la Agencia:** La Agencia revisará la propuesta y, en caso de ser aprobada, comunicará por escrito la aceptación de los nuevos miembros del equipo. Si la propuesta no cumple con los requisitos, se otorgará un plazo adicional de **10 días hábiles** para presentar alternativas.

5.3.3 Requisitos para la incorporación de nuevos perfiles

Para garantizar la calidad y continuidad del servicio, los perfiles que se incorporen al equipo tras una solicitud de cambio deberán cumplir con los mismos estándares de cualificación, experiencia y certificaciones establecidos en este pliego. A continuación, se detallan las condiciones que deben cumplir los nuevos profesionales para ser aceptados por la Agencia, asegurando que el nivel técnico y operativo del equipo no se vea afectado negativamente.

- **Cumplimiento de requisitos mínimos:** Los nuevos miembros deberán acreditar formación y certificaciones equivalentes o superiores a las exigidas en la cláusula 5.2.
- **Experiencia demostrada:** Deberán aportar experiencia relevante en auditorías de ciberseguridad o en funciones alineadas con el perfil al que sustituyen.
- **Transición sin interrupciones:** Los nuevos perfiles deberán integrarse al equipo en un plazo máximo de 15 días hábiles, garantizando la continuidad de las actividades en curso.

5.4 Obligación de desempeño en las instalaciones de la Agencia

El equipo de trabajo asignado al contrato deberá realizar sus funciones principalmente en las instalaciones de la Agencia o en la Consejería de Digitalización. Este requisito se considera esencial para garantizar la adecuada ejecución de las actividades del contrato y busca cumplir los siguientes objetivos:

- **Coordinación directa y eficiente:** Facilitar la interacción continua con las áreas técnicas, estratégicas y operativas de la Agencia, promoviendo un trabajo colaborativo y alineado con los objetivos del contrato.
- **Acceso inmediato a los recursos necesarios:** Asegurar que el equipo disponga de acceso directo a la infraestructura, documentación y herramientas necesarias para la prestación de los servicios.

El desempeño desde las instalaciones de la empresa adjudicataria será permitido únicamente en casos excepcionales, previa solicitud y autorización escrita por parte de la Agencia. Dichas excepciones deberán estar debidamente justificadas y cumplir con los siguientes requisitos:

- **Condiciones de seguridad y confidencialidad:** Las instalaciones de la empresa adjudicataria deberán garantizar medidas equivalentes o superiores a las de la Agencia para proteger la información manejada durante la ejecución del contrato.
- **Planificación previa:** La solicitud deberá incluir un plan detallado que justifique la necesidad del trabajo remoto, el tiempo estimado y las medidas de control propuestas para asegurar el cumplimiento de los estándares de calidad y confidencialidad.
- **Supervisión continua:** Durante el periodo autorizado, el adjudicatario deberá mantener una comunicación fluida con la Agencia, asegurando el cumplimiento de los plazos y objetivos establecidos.

Además, parte de la consultoría de adecuación a marco normativo podrá requerir realizarse en las entidades locales asistidas. Esto incluye cualquier trabajo relacionado con la recopilación de la situación inicial, entrevistas, o análisis de sistemas que no puedan ser efectivamente ejecutados de manera remota. La empresa adjudicataria deberá garantizar que su equipo se desplace a las instalaciones de las entidades auditadas, ubicadas en cualquier punto de la Comunidad de Madrid, asegurando el cumplimiento de los plazos y objetivos establecidos.

Se entiende que esta obligación es esencial para el adecuado desarrollo de las auditorías y no podrá ser motivo de objeción por parte del adjudicatario. En casos excepcionales, y solo con la autorización previa de la Agencia, podrían acordarse medidas alternativas para circunstancias debidamente justificadas.

CLÁUSULA 6.- TECNOLOGÍAS Y HERRAMIENTAS A UTILIZAR

6.1 Herramientas para la gestión del contrato, recursos y servicio prestado

El adjudicatario deberá implementar y utilizar herramientas tecnológicas específicas que faciliten la **gestión eficiente del contrato**, garantizando la supervisión y el control por parte de la **Agencia de Ciberseguridad**. Estas herramientas deberán proporcionar **transparencia, trazabilidad y cumplimiento** de las condiciones contractuales.

El objetivo principal es permitir el **seguimiento continuo** de la ejecución del contrato, optimizar el uso de los recursos asignados y asegurar el cumplimiento de los objetivos establecidos. Para ello, las herramientas deberán cubrir, al menos, las siguientes funciones:

- **Gestión integral del contrato:**
 - Seguimiento en tiempo real del estado de las actividades planificadas y los entregables.
 - Registro detallado de los hitos alcanzados, con indicadores asociados a las métricas de desempeño (KPIs).
 - Gestión de incidentes o desviaciones detectadas, asegurando su trazabilidad desde la notificación hasta la resolución.
- **Gestión y almacenamiento de evidencias de cumplimiento:**
 - Evidencias iniciales: Almacenamiento seguro de las evidencias que acrediten el cumplimiento de las solvencias técnicas y requisitos esenciales presentados en el momento de la adjudicación.
 - Actualización continua: Mantenimiento de la documentación actualizada durante toda la vigencia del contrato, incluyendo las certificaciones profesionales del equipo asignado, y la actualización de acreditaciones relacionadas con normativas o estándares aplicables.
- **Acceso auditable**, garantizando que la Agencia pueda revisar en cualquier momento las evidencias almacenadas para verificar su vigencia y conformidad con las condiciones del contrato.
- **Monitoreo del desempeño del equipo:**

- Registro de la dedicación y la disponibilidad del personal asignado, alineado con los requerimientos de la Cláusula 5.
- Supervisión de las horas efectivamente trabajadas y su comparación con el plan inicial de recursos.
- Control de sustituciones y justificaciones asociadas, conforme al procedimiento establecido.
- **Planificación y ajuste del programa anual de implantación de marcos normativos:**
 - Organización y actualización del programa anual de implantación de marcos normativos.
 - Revisión periódica de prioridades, objetivos y resultados intermedios, asegurando la alineación con las necesidades de la Agencia.
 - Gestión de ajustes al programa en función de cambios normativos o necesidades emergentes.
- **Supervisión de la calidad del servicio:**
 - Registro y monitoreo de la calidad de los entregables, evaluados conforme a los estándares definidos en el contrato.
 - Generación de alertas para la identificación de incumplimientos en plazos, calidad o dedicación.
 - Consolidación de métricas de desempeño para su evaluación en las reuniones de seguimiento.

6.2 Herramientas específicas de gestión GRC

El adjudicatario deberá emplear herramientas tecnológicas específicas para la gestión de **Gobierno, Riesgo y Cumplimiento**, alineadas con las mejores prácticas internacionales y los marcos normativos aplicables, incluyendo el **Esquema Nacional de Seguridad (ENS)**, la **Directiva NIS2** y las recomendaciones del **Centro Criptológico Nacional (CCN)**.

Las herramientas utilizadas por el adjudicatario deberán cubrir, al menos, las siguientes funcionalidades:

- **Gestión del Cumplimiento Normativo**
 - Evaluación del grado de alineación con el ENS, NIS2 y RGPD, permitiendo la identificación de brechas de cumplimiento y la definición de planes de acción correctivos.
 - Mantenimiento de un repositorio centralizado de normativas, políticas y procedimientos aplicables, facilitando su actualización y consulta.
 - Automatización del seguimiento de controles de cumplimiento y generación de informes de estado.
- **Gestión Integral de Riesgos**
 - Identificación y análisis de riesgos asociados a la ciberseguridad y la protección de datos, con capacidad para clasificarlos según impacto y probabilidad.
 - Priorización de riesgos y establecimiento de planes de mitigación, con trazabilidad de acciones y responsables asignados.
 - Generación de métricas e indicadores clave sobre la evolución del riesgo y la efectividad de las medidas implementadas.
- **Auditoría y Control Interno**
 - Mecanismos para la evaluación de controles internos y auditoría de conformidad con marcos normativos aplicables.

- Capacidad de almacenar y gestionar evidencias de auditoría, garantizando su trazabilidad y acceso auditable.
- Automatización de la planificación y ejecución de auditorías, facilitando la detección de desviaciones y su posterior tratamiento.
- **Gestión de Incidentes y No Conformidades**
 - Registro y categorización de incidentes de seguridad y no conformidades detectadas en auditorías.
 - Seguimiento del ciclo de vida de cada incidente, desde su identificación hasta su resolución, con asignación de responsables y plazos de respuesta.
 - Integración con mecanismos de notificación y reporte, asegurando una gestión eficiente y alineada con los requerimientos regulatorios.
- **Supervisión y Monitorización del Desempeño**
 - Generación de cuadros de mando e informes para el seguimiento de cumplimiento, riesgos e incidentes, facilitando la toma de decisiones basada en datos.
 - Trazabilidad de la evolución de los indicadores de desempeño y de los avances en la implantación de medidas correctivas.
 - Capacidad de integración con otras herramientas o sistemas empleados en la Agencia de Ciberseguridad o en las entidades auditadas.

Además de las funcionalidades mencionadas, se permitirá el uso de herramientas complementarias destinadas a tareas específicas como evaluación de riesgos, auditorías automatizadas, seguimiento del cumplimiento normativo o gestión documental, siempre que cumplan con los siguientes requisitos:

- **Compatibilidad:** Ser plenamente integrables con los sistemas utilizados por la Agencia de Ciberseguridad y las entidades auditadas.
- **Aprobación previa:** Contar con la autorización explícita de la Agencia antes de su implementación.
- **Cumplimiento normativo:** Asegurar que su uso se alinea con los estándares de seguridad de la información exigidos en el contrato.

CLÁUSULA 7.- MODELO DE GESTIÓN DEL SERVICIO

7.1 Planificación y seguimiento del servicio

La planificación y seguimiento del servicio son elementos esenciales para garantizar la correcta ejecución de las actividades contempladas en el contrato, optimizando recursos y alineando los resultados con los objetivos estratégicos de la Agencia.

7.1.1 Fases del servicio

El servicio se organizará en tres fases principales que asegurarán una ejecución eficiente y ordenada:

1. **Fase de establecimiento inicial:** Con una duración máxima de un (1) mes desde la firma del contrato, esta fase establece las bases operativas del servicio y garantiza un inicio sólido. Durante este periodo, el adjudicatario deberá:
 - **Entregar los documentos de planificación iniciales**, que incluirán:
 - a) **Plan general de trabajo** (incluyendo planificación detallada y posibles prórrogas).

- b) **Programa anual de implantación de marcos normativos**, con prioridades y cronograma detallado.
 - c) **Procedimientos de comunicación y reporte**, con frecuencia, canales y responsables.
 - **Establecer mecanismos de coordinación y comunicación con la Agencia**, incluyendo la frecuencia de reuniones, los canales de comunicación y los responsables de cada parte para garantizar una comunicación fluida.
 - **Realizar un análisis inicial de necesidades** para alinear las actividades planificadas con los objetivos estratégicos de la Agencia.
2. **Fase de servicio estabilizado:** Esta etapa, con una duración inicial de once meses, y posibilidad de prórroga, representa el núcleo operativo del contrato. Durante esta fase, el adjudicatario deberá:
- **Ejecutar el programa anual de implantación de marcos normativos**, asegurando que se alcancen los objetivos definidos por la Agencia. Esto incluye:
 - a) Planificación, ejecución, desarrollo de planes de adecuación normativo o mejora de la seguridad.
 - b) Ajustes al programa en función de los resultados obtenidos y las necesidades emergentes.
 - **Integrar el seguimiento del servicio y el avance de las adecuaciones a normativa** en las herramientas de gestión utilizadas, y reflejar los avances en informes periódicos.
 - **Participar en reuniones periódicas** con la Agencia, presentando:
 - a) Resultados de auditorías realizadas.
 - b) Progresos en la gestión de hallazgos y planes de mejora.
 - c) Propuestas para optimizar procesos y resultados.
3. **Fase de transferencia del servicio:** Esta fase comenzará dos meses antes de la finalización del contrato y estará orientada a garantizar una transición ordenada. El adjudicatario deberá:
- **Transferir toda la documentación generada**, organizada y accesible, incluyendo informes finales, resúmenes ejecutivos y datos recopilados durante la ejecución del servicio.
 - **Presentar un informe de cierre** que resuma las actividades realizadas, resultados obtenidos y recomendaciones para la continuidad y mejora de los trabajos.
 - **Colaborar con la Agencia en la entrega** de conocimientos y lecciones aprendidas, asegurando la correcta transferencia hacia futuros contratistas o responsables internos.

7.1.2 Modo de relación entre adjudicatario y Agencia

El adjudicatario deberá establecer un modelo claro y estructurado para la coordinación del servicio, basado en los siguientes elementos:

- **Funciones de gestión del Responsable de Servicio:** El Responsable del Servicio será el principal responsable de la planificación, supervisión y ejecución de las actividades, actuando como enlace entre el adjudicatario y la Agencia. Sus responsabilidades incluirán:
 - Planificación y supervisión del equipo, asegurando que cada miembro cumpla con sus responsabilidades.
 - Supervisión de plazos y calidad de los entregables, verificando que cumplan con los estándares establecidos.

- Comunicación continua con la Agencia, mediante reuniones periódicas para presentar avances y resolver incidencias, y reportes ejecutivos que detallen el progreso del servicio.
- **Comités de seguimiento:** Para garantizar un control efectivo del servicio, se constituirán los siguientes comités:
 - **Comité de Coordinación Operativa:** Revisará el progreso operativo mensual y actuará como foro para resolver incidencias específicas relacionadas con la ejecución de actividades.
 - **Comité de Seguimiento del Contrato:** Evaluará los resultados generales del servicio y propondrá ajustes estratégicos trimestralmente.
- **Instrumentos de gestión:** El adjudicatario deberá emplear herramientas y documentos que faciliten el seguimiento y control del servicio, alineadas con lo establecido en el **6.1**. Estas herramientas deberán permitir, de manera eficiente y transparente, la supervisión de las actividades realizadas y el cumplimiento de las condiciones contractuales por parte de la Agencia. En este sentido, se requerirá el uso de plataformas que posibiliten:
 - El seguimiento en tiempo real del avance del servicio, reflejando hitos alcanzados, desviaciones y acciones correctivas.
 - La gestión colaborativa entre la Agencia y el adjudicatario, asegurando una comunicación fluida y eficiente.
 - La generación y almacenamiento de informes periódicos y documentación clave, de forma accesible y organizada, para facilitar revisiones y auditorías internas.

7.2 Acuerdos de nivel de servicio (SLA) y penalizaciones

El adjudicatario deberá cumplir con los Acuerdos de Nivel de Servicio (SLAs) establecidos para garantizar la calidad, eficacia y puntualidad en la prestación de los servicios. Estos SLAs están orientados a supervisar aspectos clave del servicio, como el cumplimiento de plazos, la calidad de los entregables, la disponibilidad de los profesionales asignados al contrato y el cumplimiento del programa anual de auditorías.

La Agencia de Ciberseguridad supervisará el cumplimiento de los SLAs mediante reuniones periódicas de seguimiento y revisión de los informes de avance. Cualquier incumplimiento en el cumplimiento de estos SLAs **podrá dar lugar a la aplicación de penalizaciones**, conforme a lo establecido en el **apartado 1.18 del Pliego de Cláusulas Administrativas Particulares (PCAP)**.

Para los detalles sobre las penalizaciones aplicables en caso de incumplimientos, incluidas las cuantías y condiciones específicas, el adjudicatario deberá referirse exclusivamente al **PCAP, apartado 1.18**.

7.2.1 Cumplimiento de plazos

El adjudicatario deberá respetar los plazos establecidos para la entrega de productos, como informes técnicos, planes de mejora y demás documentación.

- **SLA:** $\geq 95\%$ de los entregables dentro de los plazos acordados.
- **Tolerancia:** Se permitirá un margen de **3 días hábiles** en entregables no críticos, siempre que no afecten la operativa del servicio.

7.2.2 Calidad de los entregables

Todos los productos entregados deberán cumplir con los estándares de calidad definidos por la Agencia. Esto incluye claridad, exhaustividad y alineación con los objetivos del contrato.

- **SLA:** $\geq 90\%$ de informes conformes a los estándares de la Agencia.

7.2.3 Disponibilidad del equipo y cumplimiento de dedicación

- **SLA:** $\geq 90\%$ de las horas mensuales exigidas, participación en reuniones críticas y respuesta a requerimientos operativos.
- **Excepciones:** Se admitirán ausencias justificadas (bajas médicas, permisos autorizados).

CLÁUSULA 8.- CONTENIDO DE LAS OFERTAS

8.1 Documentación administrativa

El licitador deberá presentar la documentación administrativa conforme a lo estipulado en el Pliego de Cláusulas Administrativas Particulares (PCAP), dentro del **Sobre nº 1**.

Esta documentación debe **limitarse exclusivamente** a los requisitos administrativos y legales establecidos, sin incluir información que pueda ser objeto de valoración técnica o económica. Se recuerda que el incumplimiento de este principio podrá conllevar la **exclusión de la licitación**, de acuerdo con la normativa vigente en materia de contratación pública.

8.2 Contenido de la oferta relativo a criterios valorables mediante juicio de valor

El **Sobre nº 2** contendrá la propuesta técnica, estructurada en secciones claramente diferenciadas y con títulos identificables.

De acuerdo con la normativa en contratación pública, queda **prohibido incluir en esta propuesta información de carácter económico**, y del resto de criterios evaluables de forma automática por aplicación de fórmulas.

8.2.1 Requisitos de redacción

La propuesta técnica deberá cumplir con los límites de extensión especificados para cada sección. Además, se establece que las ofertas técnicas deberán respetar las siguientes normas de formato:

- **Tipografía:** Arial, tamaño 11 puntos.
- **Espaciado:** Interlineado sencillo.
- **Márgenes:** 2 cm en los cuatro lados de la página.
- **Formato de página:** Tamaño A4, orientación vertical.
- **Numeración:** Las páginas deberán estar numeradas consecutivamente.
- **Portada y apartados:** Cada sección deberá comenzar en una página nueva, y se permite incluir una portada general y un índice en páginas adicionales no computables.

Adicionalmente:

- Se permite el uso de elementos visuales, como tablas o gráficos, siempre que sean legibles y estén contenidos dentro del límite de páginas indicado para cada apartado. El tamaño mínimo de fuente para contenido gráfico o tabular será de 9 puntos.
- No se permitirá incluir anexos o documentación adicional en el Sobre nº 2. Toda la información relevante debe estar contenida dentro de los apartados indicados en 8.2.2.
- Cualquier incumplimiento de las normas establecidas podrá dar lugar a la exclusión del procedimiento de licitación.

8.2.2 Estructura de la oferta

La oferta técnica relativa a los criterios evaluables mediante juicio de valor deberá presentarse estructurada de forma clara, siguiendo la misma organización y denominación empleada en los criterios de adjudicación recogidos en el Pliego de Cláusulas Administrativas Particulares (PCAP), apartado 1.8.2.

Con carácter general, la propuesta deberá ajustarse a los siguientes epígrafes y subapartados, desarrollando de forma específica los aspectos solicitados:

- **SECCIÓN I: METODOLOGÍA DE TRABAJO.** El licitador deberá describir con detalle, en un máximo de 8 páginas, la metodología propuesta para la prestación de los servicios, abordando los siguientes aspectos clave:
 - **Enfoque metodológico** para la implementación y adecuación a ENS, NIS2 y RGPD.
 - **Gestión de riesgos:** Identificación, análisis y tratamiento de riesgos alineados con estándares reconocidos.
 - **Gestión del SGSI:** Procedimientos para el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
 - **Control del cumplimiento y reporte:** Propuesta de mecanismos de control, generación de informes y trazabilidad de acciones correctivas.
- **SECCIÓN II: ORGANIZACIÓN DEL EQUIPO Y RECURSOS ASIGNADOS.** Esta sección, con un máximo de 6 páginas, deberá incluir:
 - **Estructura organizativa y roles:** Definición clara de funciones, comunicación y coordinación.
 - **Garantía de continuidad:** Plan de sustituciones para asegurar la estabilidad del servicio en caso de bajas o contingencias.
- **SECCIÓN III: PLANIFICACIÓN Y CRONOGRAMA.** El licitador deberá presentar, en un máximo de 8 páginas, un plan inicial para las tres fases del servicio (establecimiento inicial, estabilización y transferencia), incluyendo:
 - **Actividades e hitos clave:** Detalle de las principales actividades, entregables y tiempos asociados.
 - **Seguimiento y control:** Mecanismos para garantizar el cumplimiento de plazos y objetivos.
- **SECCIÓN IV: HERRAMIENTAS Y TECNOLOGÍAS PROPUESTAS.** En un máximo de 4 páginas se deberán especificar las soluciones tecnológicas que se utilizarán, incluyendo:
 - **Herramientas técnicas:** Soluciones que se emplearán en las tareas de este contrato.
- **SECCIÓN V: INDICADORES Y MECANISMOS DE SUPERVISIÓN.** El licitador deberá incluir en su propuesta, ocupando un máximo de 5 páginas, indicadores clave de rendimiento (KPIs), y detallar los mecanismos para supervisar los Acuerdos de Nivel de Servicio (SLAs), incluyendo:
 - **KPIs:** Propuesta de indicadores relevantes para medir la calidad y efectividad del servicio.
 - **Supervisión de SLAs:** Metodología para monitorear los acuerdos de nivel de servicio y gestionar incidencias operativas.

8.3 Contenido de la oferta relativo a criterios valorables mediante la aplicación de fórmulas

El **Sobre nº 3** deberá contener **exclusivamente** la **proposición económica** y cualquier otra información relacionada con los criterios evaluables mediante la aplicación de fórmulas, conforme a lo establecido en el **Pliego de Cláusulas Administrativas Particulares (PCAP)**.

Para garantizar la correcta evaluación de las propuestas, los licitadores deberán **seguir estrictamente** las indicaciones recogidas en dicho pliego y utilizar **únicamente** el modelo establecido en el **Anexo I**.

CLÁUSULA 9.- GESTIÓN DE LA SEGURIDAD

9.1 Cumplimiento de normativas

El adjudicatario deberá garantizar el estricto cumplimiento de todas las normativas aplicables a los servicios objeto del contrato. Este compromiso implica la observancia de las políticas y procedimientos definidos por la Agencia, así como el respeto a las disposiciones legales, reglamentarias y normativas en materia de **seguridad de la información, ciberseguridad y gestión de riesgos**.

En particular, se deberá cumplir con las siguientes normativas y estándares:

- **Esquema Nacional de Seguridad (ENS):** Las actividades deberán alinearse con los principios básicos y requisitos mínimos establecidos en el Real Decreto 311/2022.
- **Reglamento General de Protección de Datos (RGPD) y LOPDGDD:** Se deberán aplicar medidas técnicas y organizativas adecuadas para garantizar la protección de los datos personales tratados en el marco del contrato.
- **Disposiciones establecidas en la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, y su normativa derivada:** El adjudicatario deberá garantizar el cumplimiento de las disposiciones para el tratamiento de información clasificada, cuando estas sean exigidas a través de los reglamentos relativos a servicios esenciales e infraestructuras críticas.
- **Normativas internas de la Agencia:** El adjudicatario deberá respetar las políticas específicas de seguridad de la información y protección de datos definidas por la Agencia.

El adjudicatario será responsable de implementar las medidas de control necesarias para asegurar que sus procesos y entregables cumplan con las normativas mencionadas.

9.2 Tratamiento de datos personales

El presente contrato **no implica el tratamiento de datos personales** por parte del adjudicatario, al estar centrado en tareas de consultoría, análisis metodológico y soporte normativo que no requieren acceso a sistemas operativos ni a bases de datos que contengan datos personales.

No obstante, **en caso de que por razones operativas fuera imprescindible acceder a datos personales durante la ejecución del contrato**, se deberá comunicar previamente a la Agencia de forma expresa, a fin de valorar su legalidad y, en su caso, **formalizar el correspondiente acuerdo de encargo de tratamiento conforme al artículo 28 del RGPD**, antes de proceder a dicho acceso.

9.3 Confidencialidad

Toda la información accesible para el adjudicatario durante la ejecución del contrato será considerada estrictamente confidencial, independientemente de su naturaleza técnica, operativa o estratégica. Esto incluye, pero no se limita a:

- Datos y documentación de las entidades asistidas.
- Planes, estrategias y normativas internas de la Agencia.
- Evaluaciones, análisis de riesgos y hallazgos identificados.
- Cualquier otra información clasificada como confidencial por la Agencia.

Para esta información, las obligaciones del adjudicatario respecto a la confidencialidad son las siguientes:

1. **Firmas de acuerdos de confidencialidad:** Todos los miembros del equipo deberán firmar acuerdos específicos de confidencialidad antes de acceder a cualquier información relacionada con el contrato. Dichos acuerdos incluirán cláusulas que prohíban su uso indebido y establezcan responsabilidades en caso de incumplimiento.

2. **Medidas organizativas y técnicas:** El adjudicatario deberá implementar medidas como el almacenamiento seguro de información y el control estricto de accesos para proteger la confidencialidad durante toda la ejecución del contrato.
3. **Devolución o destrucción de información:** Al término del contrato, el adjudicatario deberá devolver toda la información confidencial en su poder o proceder a su destrucción segura, si así lo requiere la Agencia. En caso de destrucción, se deberá emitir un certificado que acredite la eliminación de los datos de manera adecuada.

Las obligaciones de confidencialidad del adjudicatario no se extinguirán con la finalización del contrato, salvo que la Agencia libere expresamente al adjudicatario de esta obligación.

El incumplimiento de estas obligaciones será considerado una infracción grave, y podrá derivar en sanciones contractuales y responsabilidades legales adicionales si se producen daños por una mala gestión de la información confidencial.

CLÁUSULA 10.- DERECHOS Y OBLIGACIONES

10.1 Propiedad de los trabajos realizados

Todos los **productos, entregables, informes y documentos** generados como resultado de los servicios prestados en el marco de este contrato serán **propiedad exclusiva** de la Agencia. Esto incluye, pero no se limita a:

- Programas anuales de cumplimiento y planes de adecuación normativa.
- Informes de evaluación y auditoría de cumplimiento.
- Planes de gestión de riesgos y tratamiento de incumplimientos.
- Recomendaciones estratégicas en materia de gobierno, riesgo y cumplimiento.
- Documentación de soporte y análisis normativos.
- Cualquier otro material derivado de las actividades del contrato.

El adjudicatario cede a la Agencia, de forma irrevocable y sin limitación temporal ni territorial, todos los derechos de explotación sobre los trabajos realizados, incluyendo, pero no limitado a:

- Derechos de reproducción
- Derechos de distribución
- Derechos de comunicación pública
- Derechos de transformación

Adicionalmente, las obligaciones del adjudicatario son las siguientes:

- **Prohibición de uso no autorizado:** El adjudicatario no podrá utilizar, reproducir, distribuir ni compartir, total o parcialmente, los trabajos realizados con terceros, salvo con autorización previa, expresa y por escrito de la Agencia. Esta prohibición incluye tanto los productos finales como los borradores, datos intermedios o cualquier otro resultado parcial de los servicios prestados.
- **Entrega de materiales al término del contrato:** En caso de finalización del contrato, ya sea por cumplimiento de su término o por resolución anticipada, el adjudicatario estará obligado a entregar a la Agencia todos los materiales, documentos y resultados generados hasta la fecha. Los materiales deberán proporcionarse en formatos editables y abiertos, tales como formatos compatibles con estándares internacionales (por ejemplo, ODF, CSV, JSON, PDF/A), que permitan su uso, modificación y adaptación sin restricciones.
- **Garantía de originalidad:** El adjudicatario deberá garantizar que los trabajos realizados son originales y no infringen derechos de terceros. En caso de reclamaciones por derechos de

propiedad intelectual, el adjudicatario asumirá toda la responsabilidad, incluyendo indemnizaciones que pudieran derivarse, y exonerará a la Agencia de cualquier perjuicio.

El incumplimiento de estas disposiciones será considerado una infracción grave y podrá dar lugar a responsabilidades legales y contractuales conforme a lo estipulado en la normativa aplicable.

10.2 Derechos sobre herramientas y software desarrollado

Cualquier herramienta, software o solución tecnológica desarrollada específicamente para la prestación de los servicios objeto del contrato será propiedad de la Agencia de Ciberseguridad de la Comunidad de Madrid, salvo disposición contraria explícita en el contrato, con las siguientes condiciones específicas:

- **Herramientas desarrolladas específicamente:** La propiedad de las herramientas o soluciones tecnológicas diseñadas para la ejecución del contrato corresponderá íntegramente a la Agencia, incluyendo los derechos de uso, modificación, distribución y mantenimiento.
- **Herramientas preexistentes del adjudicatario:** En caso de utilizar tecnologías, herramientas o soluciones de su propiedad, el adjudicatario deberá garantizar a la Agencia una licencia de uso gratuita, no exclusiva y sin limitaciones temporales, exclusivamente para actividades relacionadas con el contrato.
- **Elementos o módulos basados en software preexistente:** Si las herramientas desarrolladas incluyen elementos o módulos basados en software preexistente, el adjudicatario deberá garantizar que no existen restricciones legales o de propiedad intelectual que limiten su uso o explotación por parte de la Agencia.

El adjudicatario estará obligado a entregar toda la documentación técnica necesaria para el correcto uso y mantenimiento de las herramientas o soluciones tecnológicas desarrolladas y cuya propiedad pase a la Agencia, incluyendo:

- Manuales de usuario
- Especificaciones técnicas
- Documentos de diseño y mantenimiento
- Cualquier otro material relacionado que facilite la continuidad y sostenibilidad de las soluciones entregadas

El incumplimiento de estas disposiciones será considerado una infracción grave y podrá generar responsabilidades legales adicionales conforme a lo estipulado en el contrato y la normativa vigente.

CLÁUSULA 11.- CALIDAD DEL SERVICIO

11.1 Mecanismos de revisión y mejora continua

El adjudicatario deberá implementar un **sistema estructurado de revisión y mejora continua** para garantizar la calidad, efectividad y alineación de los servicios prestados con los objetivos de la Agencia de Ciberseguridad de la Comunidad de Madrid. Este sistema deberá incluir los siguientes elementos clave:

- **Revisión periódica del desempeño:**
 - El adjudicatario deberá realizar revisiones trimestrales del desempeño del servicio, evaluando el cumplimiento de los Acuerdos de Nivel de Servicio (SLAs) y los Indicadores Clave de Desempeño (KPIs) definidos en el contrato.
 - Las revisiones deberán incluir: Análisis detallado de las desviaciones detectadas; Identificación de causas raíz; Propuestas de mejora y medidas correctivas, priorizadas en función de su impacto; Plan de acción con responsables, plazos y recursos asignados.
- **Informes de mejora continua:**

- Al final de cada trimestre, el adjudicatario deberá presentar un informe detallado que contemple: Resultados del análisis de desempeño y evaluación comparativa con periodos anteriores; Acciones correctivas implementadas, junto con su efectividad y resultados observados; Propuestas de mejora del servicio para el siguiente periodo, incluyendo ajustes en procedimientos, metodologías y recursos.

- **Revisión conjunta con la Agencia:**

- En las reuniones trimestrales del Comité de Seguimiento del Contrato, la Agencia y el adjudicatario evaluarán conjuntamente el desempeño del servicio y las medidas de mejora propuestas.
- Estas reuniones tendrán como objetivos: Revisar la evolución del desempeño en comparación con trimestres anteriores; Ajustar prioridades estratégicas y definir nuevas metas; Identificar necesidades emergentes y proponer soluciones adaptadas a cambios en el contexto operativo; Documentar acuerdos y compromisos de mejora con plazos definidos.
- En caso de que se detecten deficiencias persistentes o incumplimientos en la aplicación de las mejoras propuestas, la Agencia podrá requerir planes de corrección específicos y establecer medidas adicionales de control.

Asimismo, los elementos definidos en esta cláusula —revisiones periódicas de desempeño, cumplimiento de SLAs y KPIs, informes de mejora continua y reuniones de seguimiento— se considerarán indicadores operativos vinculados a la calidad del servicio. Estos indicadores servirán de base tanto para la supervisión técnica del contrato como para la adopción de medidas correctoras o sancionadoras, en caso de incumplimiento. Su función es asegurar una evaluación objetiva y trazable del grado de cumplimiento del adjudicatario con respecto a las exigencias contractuales.

11.2 Evaluación de la satisfacción del cliente

La satisfacción de la Agencia con los servicios prestados será evaluada periódicamente como parte integral del proceso de supervisión y control del contrato. Para ello, se establecerán los siguientes mecanismos:

- **Encuestas de satisfacción:**

- Al menos una vez al año, el adjudicatario deberá realizar encuestas de satisfacción dirigidas a los responsables de la Agencia involucrados en el seguimiento del contrato.
- Estas encuestas deberán medir aspectos como:
 - a) La calidad y utilidad de los entregables.
 - b) Puntualidad en la ejecución de actividades.
 - c) Disponibilidad y proactividad del equipo asignado.
 - d) Eficiencia en la gestión de incidencias y propuestas de mejora.

- **Informe anual de satisfacción:**

- Basándose en los resultados de las encuestas, el adjudicatario deberá elaborar un informe anual que incluya:
 - a) Análisis detallado de los niveles de satisfacción alcanzados.
 - b) Identificación de áreas críticas o problemáticas.
 - c) Propuestas de acciones correctivas o de mejora para abordar las observaciones realizadas.
- Este informe deberá entregarse durante el primer mes del año siguiente y será discutido en una reunión de evaluación específica entre el adjudicatario y la Agencia.

- **Compromiso con la mejora:**

- Los resultados de estas evaluaciones serán incorporados al sistema de mejora continua del adjudicatario, asegurando que las observaciones y sugerencias de la Agencia se traduzcan en acciones concretas y efectivas.
- El objetivo principal de este mecanismo es mantener un nivel elevado y constante de calidad en el servicio, promoviendo una relación de colaboración proactiva entre el adjudicatario y la Agencia.

CLÁUSULA 12.- PLAZOS, DURACIÓN Y ETAPAS DE LA PRESTACIÓN

12.1 Cronograma general

El contrato tendrá una duración inicial de un año, con posibilidad de prórroga por dos periodos adicionales de un año, alcanzando una duración máxima de tres años. Durante este tiempo, se desarrollarán las siguientes fases generales de prestación del servicio:

12.1.1 Fase de establecimiento inicial

Duración: Primer mes desde la firma del contrato.

En esta fase, el adjudicatario deberá:

- **Elaborar y entregar los documentos de planificación inicial del servicio**, que incluirán como mínimo:
 - **Cronograma detallado:** Desglose temporal y organizativo de las actividades.
 - **Programa anual de implantación de marcos normativos:** Enfoque en las adecuaciones a normativa previstas para 2025.
 - **Mecanismos de gestión y supervisión:** Herramientas y metodologías para el control del servicio.
- **Coordinar reuniones iniciales con la Agencia:** Validar la planificación, establecer objetivos claros y definir los procedimientos operativos del servicio.
- **Realizar actividades preparatorias esenciales:** Incluir tareas como el establecimiento de comunicaciones, asignación de recursos y configuraciones iniciales necesarias para garantizar un inicio efectivo y eficiente del servicio.

12.1.2 Fase de servicio estabilizado

Duración: Desde el segundo mes hasta dos meses antes de la finalización del contrato.

La fase de servicio estabilizado constituye el núcleo operativo del contrato, durante la cual se ejecutarán las actividades previstas en el programa anual de implantación de marcos normativos, el seguimiento del cumplimiento de estándares de ciberseguridad y la asistencia técnica a las entidades locales de la Comunidad de Madrid.

12.1.3 Fase de transferencia del servicio

Duración: Últimos dos meses del contrato.

El adjudicatario deberá garantizar una transición ordenada y efectiva, que contemple:

- **Entrega final de todos los materiales generados:** Informes, herramientas, datos y cualquier otra documentación producida durante la ejecución del contrato, en formatos editables y abiertos.
- **Transferencia de conocimientos y capacitación:** Formación dirigida al personal técnico de la Agencia, con especial atención en el uso de herramientas y metodologías desarrolladas durante el contrato.

- **Elaboración del informe de cierre:** Este incluirá:
 - Evaluación final del servicio prestado.
 - Análisis de cumplimiento de los objetivos establecidos en el contrato.
 - Recomendaciones detalladas para la continuidad, mejora o evolución del servicio.
- **Asistencia en la transición a nuevos adjudicatarios,** si aplica: Garantizar la transferencia completa y ordenada de información y responsabilidades.

12.2 Hitos clave

El adjudicatario deberá garantizar el cumplimiento de los siguientes hitos clave durante la ejecución del contrato. El incumplimiento de estos hitos será considerado una desviación significativa, sujeta a las penalizaciones descritas en la cláusula de SLAs.

12.2.1 Hito ‘Entrega de documentos iniciales de planificación, mes 1’

Durante el primer mes de ejecución del contrato, el adjudicatario deberá elaborar y entregar los documentos iniciales de planificación.

Estos entregables serán revisados y aprobados por la Agencia, quien evaluará su viabilidad y coherencia con los objetivos contractuales. Cualquier ajuste solicitado por la Agencia deberá ser incorporado en un plazo máximo de 10 días hábiles.

12.2.2 Hitos ‘Presentación de informe trimestral de avance, final de cada trimestre’

Al cierre de cada trimestre, el adjudicatario deberá presentar un informe detallado que resuma las actividades realizadas durante el periodo. Cada informe será entregado antes del décimo día hábil del mes siguiente al cierre del trimestre y revisado por la Agencia.

12.2.3 Hito ‘Reedición del programa anual de implantación de marcos normativos, noviembre de 2025’

Durante el penúltimo mes del año 2025, el adjudicatario deberá presentar la reedición del programa anual de implantación de marcos normativos para el año 2026. Cualquier ajuste solicitado por la Agencia deberá ser incorporado en un plazo máximo de 10 días hábiles.

12.2.4 Hito ‘Primer Informe Anual Consolidado, mes 12’

Al término del primer año de ejecución del contrato, el adjudicatario deberá entregar un informe consolidado que resuma todas las actividades realizadas durante 2025, integrando:

- Un análisis detallado de los resultados obtenidos.
- El cumplimiento del programa anual de implantación de marcos normativos.
- Las lecciones aprendidas y recomendaciones estratégicas para 2026.

12.2.5 Hito ‘Reedición del programa anual de implantación de marcos normativos, noviembre de 2026’

En caso de ejecutar prórrogas, el adjudicatario deberá presentar durante el penúltimo mes de 2026 la reedición del programa anual de implantación de marcos normativos para 2027.

Este programa deberá ser entregado a la Agencia para su revisión y aprobación antes del término de noviembre de 2026. Los ajustes solicitados deberán ser incorporados en un plazo máximo de 10 días hábiles.

12.2.6 Hito 'Reedición del programa anual de implantación de marcos normativos, noviembre de 2027'

En caso de ejecutar prórrogas, el adjudicatario deberá presentar durante el penúltimo mes de 2027 la reedición del programa anual de implantación de marcos normativos para 2028.

Este programa deberá ser entregado a la Agencia para su revisión y aprobación antes del término de noviembre de 2027. Los ajustes solicitados deberán ser incorporados en un plazo máximo de 10 días hábiles.

12.2.7 Hito 'Transferencia del servicio'

Durante los últimos dos meses del contrato, el adjudicatario deberá garantizar una transición ordenada y efectiva del servicio. Esto incluye:

- La entrega final de todos los productos, documentos y resultados generados durante la ejecución del contrato, en formatos editables.
- La realización de sesiones de transferencia de conocimientos y capacitación para el personal técnico de la Agencia.
- La disposición de asistencia técnica para resolver dudas o problemas durante el proceso de transferencia.

CLÁUSULA 13.- GARANTÍA DE LOS TRABAJOS

El adjudicatario garantizará los trabajos realizados durante un período mínimo de **12 meses**, contados a partir de la **fecha de recepción formal y conformidad expresa** por parte de la Agencia de los entregables objeto del contrato.

Durante dicho período de garantía, el adjudicatario deberá subsanar sin coste adicional alguno cualquier error, deficiencia o desviación detectada en los entregables, informes, análisis o recomendaciones formuladas, siempre que dichas incidencias no sean atribuibles a cambios sobrevenidos en el entorno normativo o tecnológico.

Asimismo, si se identifican incumplimientos de requisitos técnicos o funcionales especificados en el contrato, el adjudicatario deberá corregirlos en un plazo máximo de 10 días hábiles desde su notificación por parte de la Agencia. En caso de no hacerlo, podrá ser objeto de penalidades conforme al régimen establecido en este pliego.

Este plazo de garantía será exigible aunque el contrato haya finalizado, y se entenderá sin perjuicio de la posible exigencia de responsabilidades derivadas de daños o perjuicios ocasionados por deficiencias imputables al adjudicatario.

CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO TÉCNICO

Durante el periodo de presentación de la oferta y, ante cualquier duda o necesidad de aclaración referida a las especificaciones del Pliego de Prescripciones Técnicas, el licitador podrá dirigirse a:

Agencia de Ciberseguridad de la Comunidad de Madrid

Licita_Agencia_Ciber@madrid.org

*Área Técnica, Operaciones y Transformación
Ciberseguridad*

M^a ISABEL GONZALEZ
CENTENERA - DNI [REDACTED]
Firmado digitalmente por M^a
ISABEL GONZALEZ CENTENERA
- DN [REDACTED]
Fecha: 2025.04.15 14:12:52
+02'00'

Dña. María Isabel González Centenera

Conforme,

*El Consejero Delegado de la Agencia de
Ciberseguridad de la Comunidad de Madrid*

D. Alejandro Las Heras Vázquez

Firmado digitalmente por: ALEJANDRO LAS HERAS VÁZQUEZ - [REDACTED]
Fecha: 2025.04.15 16:17
Verificación y validez por [REDACTED]. La autenticidad de este
documento se puede comprobar en www.madrid.org/csv.