

**SISTEMA DINÁMICO DE ADQUISICIÓN DE SERVICIOS DIRIGIDOS AL
DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA, DEL SISTEMA
ESTATAL DE CONTRATACIÓN CENTRALIZADA - SDA 26/2021**

(Expediente nº 2021/16)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

**SERVICIO DE CONSULTORÍA TÉCNICA ESPECIALIZADA
PARA EL AVANCE DEL CUMPLIMIENTO NORMATIVO EN
APOYO AL DESARROLLO DE LA ADMINISTRACIÓN
ELECTRÓNICA DE ENTIDADES LOCALES**

(Exp. ACR-003-2026)

En virtud de lo dispuesto en el artículo 226 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que transponen al ordenamiento jurídico español las directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, se invita a todas las empresas admitidas al sistema dinámico de adquisición a presentar oferta en la licitación de este contrato específico en el plazo máximo de **10 días desde el día siguiente al envío de esta invitación**. La oferta deberá ajustarse a lo establecido en los pliegos que rigen el sistema dinámico de adquisición y a los términos y condiciones que se concretan en esta invitación.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

TÉRMINOS Y CONDICIONES

1.	ORGANISMO DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO	5
2.	TITULO Y OBJETO DEL CONTRATO ESPECÍFICO.....	5
3.	DURACIÓN DEL CONTRATO Y PRÓRROGA	6
3.1.	Plazo de ejecución del contrato	6
3.2.	Prórroga del contrato específico.....	6
4.	VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN	6
4.1.	Presupuesto de licitación y aplicaciones presupuestarias	6
4.2.	Tramitación del expediente (a efectos presupuestarios).....	7
4.3.	Sistema de determinación del precio	7
4.4.	Valor estimado.....	7
4.5.	Contrato financiado con cargo al presupuesto de la Unión Europea.....	13
4.6.	Modificación del contrato específico	13
5.	LUGAR DE PRESTACIÓN DE LOS SERVICIOS	13
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN.....	13
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	14
7.1.	PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN	14
7.2.	Criterios cuya cuantificación depende de un juicio de valor.....	14
7.2.1.	Criterios y ponderación.....	14
7.2.2.	Método de valoración y documentación	15
7.3.	Precio de la oferta.....	16
7.4.	Otros criterios automáticos evaluables mediante fórmulas, distintos al precio.....	17
7.5.	Fórmulas aplicables a los criterios automáticos evaluables mediante fórmulas	18
7.6.	Aplicación del umbral del 50% de puntuación	18
8.	OFERTAS ANORMALMENTE BAJAS	19
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA.....	19
9.1.	Obligaciones generales	19
9.2.	recursos a aportar al servicio	20
9.2.1.	Definición del equipo mínimo u orientativo	20
9.2.2.	Adscripción de medios personales o materiales	22
9.2.3.	Documentación justificativa de disponer de los medios a que se hubiese comprometido a dedicar o adscribir al contrato	22
9.2.4.	CONSTITUCIÓN DEL EQUIPO DE TRABAJO	22
9.2.5.	Régimen de sustitución del personal	22
9.3.	Esquema Nacional de Seguridad.....	22
9.4.	Otras condiciones de ejecución del contrato.....	23
10.	PAGO DE LOS SERVICIOS Y FACTURACIÓN	23



10.1.	Condiciones de presentación de las facturas	24
11.	PLAZO DE GARANTÍA DEL OBJETO DEL SERVICIO	25
12.	PENALIDADES	25
12.1.	Penalidades fijadas en el sistema dinámico de adquisición	25
12.2.	Fórmula para la aplicación de penalidades	25
13.	CAUSAS DE RESOLUCIÓN DE LOS CONTRATOS ESPECÍFICOS.....	25
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS.....	26
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	29
1.	RÉGIMEN JURÍDICO APLICABLE	30
2.	COMPONENTE E INVERSIÓN Y COMPROMISOS ASUMIDOS POR LA CONTRIBUCIÓN AL ETIQUETADO VERDE Y DIGITAL Y POR EL PRINCIPIO DE NO CAUSAR DAÑO SIGNIFICATIVO AL MEDIOAMBIENTE (DNSH).....	31
3.-	CLÁUSULA DE MODIFICACIÓN DE LOS CONTRATOS BASADOS FINANCIADOS EN EL PRTR.....	31
4.-	PENALIDADES POR EJECUCIÓN DEFECTUOSA O INCORRECTA EJECUCIÓN DE LOS CONTRATOS BASADOS FINANCIADOS EN EL PRTR.....	32
5.-	OBLIGACIONES DE ACREDITACIÓN PARA LOS LICITADORES, CONTRATISTAS Y SUBCONTRATISTAS ESTABLECIDAS EN EL PRTR	32
	ANEXO I DESCRIPCIÓN DEL ENTORNO TÉCNICO Y FUNCIONAL EXISTENTE	36
I.1.	Descripción de los sistemas de información existentes	36
I.2.	Descripción del entorno tecnológico.....	36
	ANEXO II DEFINICIÓN Y ALCANCE DE LOS TRABAJOS.....	36
II.1.	Requisitos funcionales	39
2.1	Evaluación de preparación para auditoría (pre-auditoría técnica)	40
2.2	Auditoría interna completa	41
2.3	Apoyo a auditoría de certificación externa por terceros	42
2.4	Validación de acciones correctoras y cierres de hallazgos	42
3.1	Dinamización de Comités de Seguridad locales	44
3.2	Reforzamiento del Comité de Seguridad de la Información de la Comunidad	44
II.2.	Requisitos no funcionales	45
II.2.1.	requisitos técnicos	45
II.2.2.	Metodología.....	45
II.2.3.	Calidad de los desarrollos	46
II.2.4.	Gestión del proyecto.....	46
II.3.	Hitos y entregables	46
	ANEXO III Servicios de mantenimiento para asegurar la continuidad de sistemas en entornos productivos.....	48
III.1.	Descripción del servicio de mantenimiento para aseguramiento de la continuidad del servicio de los sistemas en entornos productivos	49
III.2.	Dimensionamiento del servicio.....	49
III.3.	Acuerdos de nivel de servicio.....	49
	ANEXO IV MODELO DE GESTIÓN Y DEFINICIÓN DE UNIDADES DE TRABAJO	49
	ANEXO V REQUISITOS DE LOS PERFILES PROFESIONALES	49
	ANEXO VI CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD	52
	ANEXO VII MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN	55



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

1. ORGANISMO DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO

Organismo destinatario

Unidad proponente: **La Agencia de Ciberseguridad de la Comunidad de Madrid**

Centro directivo: **La Agencia de Ciberseguridad de la Comunidad de Madrid**

Departamento/organismo: **La Agencia de Ciberseguridad de la Comunidad de Madrid**

Responsable del contrato: Alejandro Las Heras Vázquez, Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid

Datos de contacto:

Dirección Postal: **Calle Embajadores, 181 – 28045 Madrid**

Correo electrónico: Licita_Agencia_Ciber@madrid.org

Teléfono: **91.580.50.01**

Órgano de Contratación:

- **La Agencia de Ciberseguridad de la Comunidad de Madrid**

2. TITULO Y OBJETO DEL CONTRATO ESPECÍFICO

Título del contrato: SERVICIO DE CONSULTORÍA TÉCNICA ESPECIALIZADA PARA EL AVANCE DEL CUMPLIMIENTO NORMATIVO EN APOYO AL DESARROLLO DE LA ADIMINSTRACIÓN ELECTRÓNICA DE ENTIDADES LOCALES

Objeto del contrato: El presente contrato tiene por objeto la prestación de un servicio de consultoría técnica especializada en materia de seguridad de la información y cumplimiento del Esquema Nacional de Seguridad (ENS), destinado a reforzar la gestión y gobernanza de la seguridad en los sistemas de información de las entidades locales de la Comunidad de Madrid que tienen menos de 20.000 habitantes.

El servicio se enmarca en las actuaciones de apoyo al desarrollo de la administración electrónica, comprendiendo tareas de análisis, planificación y asistencia técnica para la implantación y armonización de un modelo común de gestión de la seguridad de la información (SGSI-ENS).

CLASIFICACIÓN

- (X) a. La prestación consiste en la realización de trabajos según los requisitos funcionales, requisitos no funcionales e hitos y entregables del **ANEXO II** de la presente invitación.
- () b. La prestación comprende trabajos de mantenimiento de duración determinada conforme a los acuerdos de nivel de servicio en base a los que se efectúa la facturación de la prestación definidos en el **ANEXO III**.
- () c. Los servicios de desarrollo y mantenimiento de aplicaciones informáticas se definen en los términos previstos en el artículo 308.3 de la LCSP y conforme al **ANEXO IV**.

TRATAMIENTO DE DATOS PERSONALES

(X) El contrato **NO** requiere tratamiento de datos personales

() El contrato **SI** requiere tratamiento de datos personales,



La finalidad para la que se ceden los datos es: No aplica

3. DURACIÓN DEL CONTRATO Y PRÓRROGA

3.1. PLAZO DE EJECUCIÓN DEL CONTRATO

Plazo de ejecución del contrato: CUATRO (4) meses

El plazo del **contrato específico** se iniciará:

(☒) Al día siguiente, a partir de la notificación de la adjudicación del contrato.

(☐) El _____ salvo que la adjudicación del contrato específico se produzca el mismo día o con posterioridad a dicha fecha, en cuyo caso será la fecha siguiente a la notificación de la adjudicación del contrato específico.

3.2. PRÓRROGA DEL CONTRATO ESPECÍFICO

El presente contrato específico:

(☒) **No es prorrogable.** Sin perjuicio de la posibilidad de ampliación del plazo de ejecución descrita en el artículo 29.3 de la LCSP.

(☐) **Sí es prorrogable**, en las siguientes condiciones:

- Se prevé una única prórroga, manteniendo inalterables las características del contrato específico durante la misma. Esta prórroga sólo podrá ser ejecutada mientras el sistema dinámico de adquisición siga en vigor y la empresa adjudicataria esté admitida en el mismo en el momento de formalizarla.
- La prórroga será obligatoria para el contratista, cuando su preaviso se produzca en los términos establecidos en el artículo 29.2 de la LCSP.
- Duración de la prórroga: ____
- Plazo de preaviso en los términos del artículo 29.2 de la LCSP: **2 meses**

4. VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN

4.1. PRESUPUESTO DE LICITACIÓN Y APLICACIONES PRESUPUESTARIAS

Presupuesto sin IVA (€)	IVA (€)	Presupuesto con IVA (€)
214.088,75 €	44.958,64 €	259.047,39 €

Las obligaciones económicas que se deriven para la Administración por el cumplimiento del contrato serán financiadas por el Presupuesto de Gastos del organismo “*Agencia de Ciberseguridad de la Comunidad de Madrid*”, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	2026	TOTAL
“SERVICIO DE CONSULTORÍA TÉCNICA ESPECIALIZADA PARA EL AVANCE DEL CUMPLIMIENTO NORMATIVO EN APOYO AL DESARROLLO DE LA ADIMINSTRACIÓN ELECTRÓNICA DE ENTIDADES LOCALES”	259.047,39 €	259.047,39 €



4.2. TRAMITACIÓN DEL EXPEDIENTE (A EFECTOS PRESUPUESTARIOS)

(☒) Ordinaria.

(☐) Anticipada:

Se hace constar que el plazo de ejecución comenzará a partir del _____, y que la adjudicación del contrato queda sometida a la condición suspensiva de existencia de crédito adecuado y suficiente para financiar las obligaciones derivadas del contrato en el ejercicio correspondiente, de acuerdo con el artículo 117.2 de la LCSP y la normativa contable de aplicación.

4.3. SISTEMA DE DETERMINACIÓN DEL PRECIO

De acuerdo con los artículos 102.4 y 309 de la LCSP, la determinación del precio del contrato se realiza:

(☐) A tanto alzado

PRESTACIONES 2.a)	PRESTACIONES 2.b)
<i>Definir %</i>	<i>Definir %</i>

(☒) Por precios unitarios

4.4. VALOR ESTIMADO

Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **DOSCIENTOS CATORCE MIL OCHENTA Y OCHO EUROS CON SETENTA Y CINCO CÉNTIMOS**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	214.088,75 €
Importe máximo por modificación prevista, sin IVA	0 €
Importe máximo de la eventual prórroga, sin IVA (*)	0 €
TOTAL	214.088,75 €

El contrato, conforme a los umbrales establecidos en la normativa contractual:

(☐) **SI** está sujeto a regulación armonizada

(☒) **NO** está sujeto a regulación armonizada

En el cálculo del valor estimado se han tenido en cuenta los costes derivados de la aplicación de las normativas laborales vigentes, considerado los costes de personal que deberán encargarse de ejecutar la prestación.

El convenio colectivo sectorial de aplicación en los términos indicados es el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública, publicado mediante Resolución de 4 de abril de 2025, de la Dirección General de Trabajo, por la que se registra y publica el citado Convenio. No consta que exista diferencia por género en el Convenio colectivo que resulta de aplicación.

Igualmente se han considerado otros costes que se deriven de la ejecución material de los servicios, los gastos generales de estructura, otros costes indirectos y el beneficio industrial. A continuación, se detallan los conceptos y se justifican los porcentajes aplicados:

- **Costes Directos (CD):** Corresponden al coste asociado al personal necesario para la ejecución del contrato. Incluyen los salarios base establecidos en el **XIX Convenio colectivo**



estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública, incrementados por la especialización exigida en consultoría de seguridad de la información y ciberseguridad, las cargas sociales, y otros conceptos asociados de manera directa al profesional.

- **Resto Costes Directos (RCD):** Incluye los costes adicionales asociados al profesional en la ejecución del contrato, y responde a tres componentes esenciales: **equipamiento, formación especializada y provisión por indemnización.**

- Equipamiento y Herramientas de Trabajo:

- Infraestructura informática especializada: Herramientas avanzadas de evaluación de vulnerabilidades, análisis forense digital, test de penetración y gestión de riesgos.
- Soluciones de conectividad y seguridad: Acceso seguro a redes, VPN corporativas, autenticación multifactor (MFA), equipos móviles y cifrado de comunicaciones.

- Formación Especializada y Certificaciones:

- Ciberseguridad y normativas internacionales: Mantenimiento de certificaciones como CISA, CISM, CISSP, ISO 27001 Lead Auditor, DPO certificado, ENS Auditor.
- Actualización constante: Cursos, seminarios y conferencias para enfrentar amenazas emergentes.

- Provisión por Indemnización y Costes de Rotación:

- Costes de despido o finalización de contrato: La legislación laboral prevé indemnizaciones que deben ser presupuestadas.
- Impacto de la rotación en ciberseguridad: La alta demanda en el sector genera costes de selección y formación en caso de cambios en el equipo.

Dado que los costes aquí descritos pueden fluctuar, los ajustes se equilibran dentro del 14% de costes indirectos y generales, garantizando que el presupuesto cubre adecuadamente todas las necesidades del contrato.

- **Costes indirectos + Gastos generales:** Este concepto, calculado como el **14% de los costes directos**, engloba los costes que no pueden imputarse directamente a una única actividad o recurso del proyecto, pero que son esenciales para la correcta ejecución del servicio. Incluye las siguientes partidas:

- **Gastos administrativos generales:** costes de gestión y administración asociados al cumplimiento de las obligaciones fiscales, contables y de supervisión de la actividad mercantil.
- **Infraestructura corporativa y servicios de soporte:** costes asociados a oficinas, electricidad, climatización, limpieza, acceso a internet corporativo, seguridad física de las instalaciones y mantenimiento de infraestructuras.
- **Servicios de ciberseguridad transversales:** implementación y mantenimiento de medidas de seguridad informática obligatorias para garantizar la protección de la información tratada en el contrato, como cortafuegos, segmentación de red, autenticación reforzada y sistemas de monitorización de eventos de seguridad.
- **Licencias y certificaciones de cumplimiento** de la organización, que habilita o capacita para la realización de los trabajos: suscripciones a marcos normativos (ISO 27001, NIST, ENS) y herramientas necesarias para cumplir con auditorías y revisiones de seguridad.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

- **Seguros de responsabilidad civil y ciberseguridad:** pólizas necesarias para cubrir posibles riesgos de responsabilidad profesional y ciberataques que puedan impactar en la ejecución del servicio.
- **Auditoría y control de calidad:** procedimientos de supervisión interna para asegurar la correcta ejecución del contrato y la entrega de resultados conforme a los estándares de la industria.

El porcentaje aplicado se ajusta a las prácticas habituales de contratación en proyectos de consultoría y auditoría en ciberseguridad, donde estos elementos son críticos para garantizar un entorno de trabajo seguro y conforme a la normativa vigente.

- **Beneficio empresarial:** Calculado como el **6% de los costes directos**, representa el margen de beneficio neto de la empresa adjudicataria. Este margen es coherente con los estándares del sector, considerando que los proyectos de ciberseguridad requieren **inversión en tecnología avanzada, formación continua del personal y adaptación a cambios normativos constantes**.

El desglose de los costes directos e indirectos y otros eventuales gastos calculados para la determinación del presupuesto base de licitación, en aplicación del artículo 100.2 de la LCSP, es el siguiente:

Desglose Precio	
Costes directos	
Personal	162.188,44 €
Resto costes directos	16.218,84 €
Costes indirectos + Gastos generales + Beneficio industrial	35.681,46 €
Total, sin IVA	214.088,75 €

En cuanto a los costes directos de **personal** la estimación a partir del XIX Convenio colectivo estatal de empresas de consultoría (Resolución de 4 de abril de 2025, de la Dirección General de Trabajo), en función de la dedicación del personal asignado a la ejecución del contrato es:

Costes de personal							
Perfiles	Dedicación	Salario según convenio (€)	Especialización tecnológica ¹	Salario anual (€)	Coste anual según dedicación (€)	Coste personal contrato (€)	Coste personal contrato con Seguridad Social 30%
Jefe de Proyecto (Especialidad Seguridad)	50%, durante 4 meses	31.021,24	250%	77.553,10	38.776,55	12.925,52	16.803,17
Consultor (Especialidad Seguridad)	300%, durante 4 meses	30.853,02	210%	64.791,34	194.374,03	64.791,34	84.228,74
Consultor (Cumplimiento Legal)	100%, durante 4 meses	29.949,83	200%	59.899,66	59.899,66	19.966,55	25.956,52
Analista (Especialidad Seguridad)	300%, durante 4 meses	27.076,93	100%	27.076,93	81.230,79	27.076,93	35.200,01
						162.188,44 €	

¹ Se requiere personal con conocimientos, habilidades y destrezas específicos que conllevan que el personal que posee dichas competencias técnicas esté especialmente reconocido y valorado en el mercado laboral. (justificación e indicación del origen de la estimación realizada contenida en este documento).



Si bien resulta de aplicación el Convenio sectorial, en el presente servicio se requiere una cualificación superior debido a la alta especialización, experiencia y requisitos exigidos para la correcta ejecución del contrato.

Dada la complejidad y criticidad del ámbito de auditoría de seguridad de la información y ciberseguridad, los incrementos responden a la necesidad de contar con perfiles altamente cualificados, con certificaciones y experiencia en normativas específicas como el Esquema Nacional de Seguridad (ENS), NIS2, RGPD e ISO/IEC 27001. La alta demanda y escasa oferta de estos profesionales en el mercado refuerza la necesidad de ofrecer remuneraciones competitivas, alineadas con la complejidad y responsabilidad de las funciones desempeñadas.

A continuación, se detallan los cálculos y justificaciones del incremento sobre el salario base según convenio.

- Jefe de Proyecto (Especialidad Seguridad):
 - **Categoría:** Área 4, A1.
 - **Salario base según convenio:** 31.021,24€
 - **Incremento aplicado:** 250%. Este perfil corresponde a un experto con liderazgo en auditoría de seguridad, cuya responsabilidad principal es la dirección de los trabajos de auditoría, la coordinación de equipos multidisciplinares y la toma de decisiones estratégicas en materia de ciberseguridad. La justificación del incremento salarial se fundamenta en los siguientes factores:
 - Alta especialización y certificaciones avanzadas: Se requiere que el profesional cuente con certificaciones como CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager) o CISA (Certified Information Systems Auditor), exigidas en auditorías de seguridad de nivel estratégico.
 - Dirección y ejecución de auditorías de alto nivel: Las auditorías en ciberseguridad requieren una gestión experta, en cumplimiento con el Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y el RGPD. Estas normativas establecen requisitos estrictos para la evaluación de la seguridad en organismos públicos.
 - Experiencia en la gestión de riesgos y gobernanza de la seguridad: La ISO/IEC 27005 establece un marco específico para la gestión de riesgos en seguridad de la información, el cual debe ser liderado por profesionales con conocimientos en metodologías como MAGERIT.
 - Coordinación de equipos de auditoría multidisciplinares: La función de liderazgo implica gestionar equipos compuestos por especialistas técnicos, legales y operacionales, asegurando una correcta ejecución de auditorías que cubran aspectos normativos, tecnológicos y organizativos.
 - **Salario ajustado:** 77.553,10€.
 - **Coste directo de personal anual según dedicación** (sin incrementos por conceptos de Seguridad Social): 38.776,55 €.
 - **Coste de personal en la duración del contrato**, sin prórrogas (4 meses) ni conceptos de Seguridad Social: 12.925,52 €.



- Consultor (Especialidad Seguridad):

- **Categoría:** Área 4, B1.
- **Salario base según convenio:** 30.853,02€.
- **Incremento aplicado:** 210%. Este perfil corresponde a un especialista con habilidades técnicas avanzadas en ciberseguridad y de medidas técnicas y organizativas alineadas con el cumplimiento de la legislación aplicable. El incremento salarial responde a la necesidad de contar con expertos en:
 - Evaluación de riesgos tecnológicos y auditoría de sistemas: Las normativas internacionales como la ISO/IEC 27001 e ISO/IEC 27002 requieren profesionales con un profundo conocimiento de controles de seguridad, evaluación de riesgos y protección de infraestructuras críticas.
 - Especialización en modelos de gobernanza de ciberseguridad, incluyendo roles, responsabilidades, políticas, procedimientos y métricas alineadas con marcos como ISO 27001, NIST y ENS.
 - Experiencia demostrable en la realización de adaptaciones al ENS, incluyendo la elaboración de documentación parte del SGSI, así como la realización de análisis de cumplimiento preliminares y apoyo en la aplicación de acciones de remediación sobre las debilidades encontradas.
- **Salario ajustado:** 64.791,34 €.
- **Coste directo de personal anual según dedicación** (sin incrementos por conceptos de Seguridad Social): 194.374,03€.
- **Coste de personal en la duración del contrato**, sin prórrogas (4 meses) ni conceptos de Seguridad Social: 64.791,34 €.

- Consultor (Cumplimiento Legal):

- **Categoría:** Área 4, B2.
- **Salario base según convenio:** 29.949,83 €.
- **Incremento aplicado:** 200%. Este perfil se enfoca en la auditoría normativa y el cumplimiento legal en ciberseguridad. La justificación del incremento salarial radica en:
 - Responsabilidad en auditorías de cumplimiento regulatorio: La complejidad de las auditorías basadas en el ENS, NIS2, RGPD y normativa sectorial demanda conocimientos especializados en legislación aplicable a seguridad de la información.
 - Necesidad de conocimientos avanzados en normativas de seguridad: La evolución del marco regulatorio europeo y nacional hace indispensable que el profesional domine aspectos de privacidad, protección de datos, soberanía digital y continuidad de negocio.
 - Participación en la redacción y revisión de normativas internas y procedimientos de seguridad: Además de realizar auditorías, este perfil contribuye a la adaptación de las normativas de seguridad de las entidades públicas a los nuevos requisitos legales y técnicos, asegurando su alineación con los estándares más recientes.



- **Salario ajustado:** 59.899,66 €.
- **Coste directo de personal anual según dedicación** (sin incrementos por conceptos de Seguridad Social): 59.899,66 €.
- **Coste de personal en la duración del contrato**, sin prórrogas (4 meses) ni conceptos de Seguridad Social: 19.966,55 €.
- Analista (Especialidad Seguridad):
 - **Categoría:** Área 4, C2.
 - **Salario base según convenio:** 27.076,93 €.
 - **Incremento aplicado:** Sin incremento, acorde a su perfil de entrada, orientado a apoyar tareas de auditoría bajo supervisión.
 - **Salario ajustado:** 27.076,93 €.
 - **Coste directo de personal anual según dedicación** (sin incrementos por conceptos de Seguridad Social): 81.230,79 €.
 - **Coste de personal en la duración del contrato**, sin prórrogas (4 meses) ni conceptos de Seguridad Social: 27.076,93 €.

Por otra parte, el desarrollo de los trabajos requiere de **otros costes directos adicionales asociados al profesional en la ejecución del contrato, y responde a tres componentes esenciales: equipamiento, formación especializada y provisión por indemnización**, cuyo presupuesto asciende a 16.737,94 €. Los conceptos estimados son los siguientes:

- **Equipamiento y Herramientas de Trabajo:**
 - Infraestructura informática especializada: Herramientas avanzadas de evaluación de vulnerabilidades, análisis forense digital, test de penetración y gestión de riesgos.
 - Soluciones de conectividad y seguridad: Acceso seguro a redes, VPN corporativas, autenticación multifactor (MFA), equipos móviles y cifrado de comunicaciones.
- **Formación Especializada y Certificaciones:**
 - Ciberseguridad y normativas internacionales: Mantenimiento de certificaciones como CISA, CISM, CISSP, ISO 27001 Lead Auditor, ENS Auditor.
 - Actualización constante: Cursos, seminarios y conferencias para enfrentar amenazas emergentes.
- **Provisión por Indemnización y Costes de Rotación:**
 - Costes de despido o finalización de contrato: La legislación laboral prevé indemnizaciones que deben ser presupuestadas.
 - Impacto de la rotación en ciberseguridad: La alta demanda en el sector genera costes de selección y formación en caso de cambios en el equipo.



Conforme a lo establecido en el artículo 103 de la LCSP, no procederá la revisión de precios durante la vigencia del contrato.

4.5. CONTRATO FINANCIADO CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA

() No.

(X) Sí. Instrumento /Fondo/Programa/Mecanismo: **Plan de Recuperación, Transformación y Resiliencia - financiado por la Unión Europea – Next Generation EU**

Código de operación/Proyecto/Iniciativa: **C15.I07.P06.S61.PROVISIONAL.SI01**

Corresponde al organismo destinatario o, en su caso, al organismo financiador del presente contrato específico, la acreditación de todos los requisitos que resulten exigibles por la normativa comunitaria o nacional para obtener el retorno de las ayudas europeas. Resultan de obligado cumplimiento al presente contrato las obligaciones establecidas en la Adenda para contratos cofinanciados para las partes.

4.6. MODIFICACIÓN DEL CONTRATO ESPECÍFICO

Este contrato específico no podrá ser modificado durante su vigencia en los supuestos de modificación legal contemplados en el artículo 205 de la LCSP y en los supuestos del epígrafe 27.18 del PCAP.

Serán de aplicación las siguientes condiciones: **NO APLICA.**

5. LUGAR DE PRESTACIÓN DE LOS SERVICIOS

() La prestación de los servicios de desarrollo se efectuará en la sede de la Administración

(X) La ejecución de las tareas de desarrollo se realizará, como regla general, en la sede del adjudicatario, salvo aquellas tareas relacionadas con la recogida de requisitos, implantación y puesta en marcha u otras similares en las que resulte más conveniente para una mejor ejecución de los trabajos.

En todo caso, el Coordinador Técnico del Contrato está obligado a acudir a la ubicación designada por la entidad destinataria del contrato específico siempre que ésta así lo solicite.

() El adjudicatario puede ofertar la realización de las tareas en modalidad no presencial según plan de ejecución de teletrabajo.

() Otra opción

6. INCOMPATIBILIDADES PARA LA LICITACIÓN

(X) **No ha existido participación de empresas** en la elaboración de las especificaciones técnicas o los documentos preparatorios del contrato específico ni existen incompatibilidades por causas de la naturaleza de los trabajos

() **Sí han participado empresas** en la elaboración de especificaciones técnicas o de los documentos preparatorios del contrato específico

En este caso se han adoptado las siguientes medidas para garantizar que su participación en la licitación no falsee la competencia:



() **Comunicación** a los demás candidatos o licitadores de la información intercambiada en el marco de la participación en la preparación del procedimiento de contratación o como resultado de ella, y establecimiento de plazos adecuados para la presentación de ofertas

() Otras:

() Existen incompatibilidades por causas de la naturaleza de los trabajos.

7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN

El presente contrato tiene por objeto prestaciones de carácter intelectual:

() No

(X) Sí

7.1. PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN

1. Ponderación de los criterios según forma de evaluarlos

SOBRE 1. Criterios que dependen de un juicio de valor	SOBRE 2. Criterios evaluables mediante fórmulas
49%	51%

2. Ponderación entre criterios cualitativos y criterios relacionados con el precio si el contrato tiene por objeto **prestaciones de carácter intelectual**

Criterio precio	Otros criterios automáticos	Criterios no automáticos
40%	11%	49%

7.2. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

7.2.1. CRITERIOS Y PONDERACIÓN

CRITERIO	PONDERACIÓN EN PUNTOS (SOBRE 100)
Solución técnica ofertada (arquitectura, comprensión de los requisitos, viabilidad, metodología, rendimiento previsible, satisfacción de los requisitos...)	60
Planificación del servicio (calendario, horario, análisis de riesgos, plan de contingencias, plan de calidad, trazabilidad del servicio...)	40



7.2.2. MÉTODO DE VALORACIÓN Y DOCUMENTACIÓN

Criterios sujetos a un juicio de valor (49% del peso global)

A continuación, se especifica para cada criterio basado en juicio de valor los aspectos que se valoran y el baremo relativo de cada uno. Estos criterios tienen un peso conjunto del 49% sobre la valoración total.

1. Solución técnica ofertada (60 puntos)

Se evaluará la calidad, claridad y coherencia de la propuesta metodológica presentada por la empresa licitadora para la prestación del servicio de soporte especializado en auditoría. Se valorará especialmente:

- La comprensión de los objetivos y necesidades del contrato, en relación con el apoyo técnico y documental a la implantación efectiva de un sistema común de gestión de la seguridad de la información (SGSI) en el entorno local de la Comunidad de Madrid.
- La adecuación del enfoque metodológico propuesto a los marcos normativos aplicables, especialmente ENS.
- El grado de estructuración y aplicabilidad de la propuesta, incluyendo mecanismos de interacción con la Agencia de Ciberseguridad.
- La utilización de herramientas técnicas y recursos documentales que aporten eficiencia, trazabilidad y valor añadido a las tareas descritas.
- La capacidad de la propuesta para adaptarse al entorno local objeto del contrato.

Baremo de valoración:

- 10 puntos (Excelente): Propuesta altamente detallada, con soluciones innovadoras, perfectamente adaptadas a los objetivos del contrato. Demuestra un profundo conocimiento del contexto del proyecto, con una metodología coherente y adaptada a las necesidades específicas.
- 7 puntos (Muy bueno): Propuesta bien contextualizada, estructurada y coherente, aunque con áreas mejorables en el detalle o concreción en algunas fases del proyecto. Muestra un buen nivel de adecuación, aunque no destaca por su carácter innovador.
- 5 puntos (Adecuado): Propuesta funcional, aunque genérica y con carencias significativas en la estructura o detalle de la metodología. Se limita a cumplir los requisitos del pliego, sin una adaptación evidente al contexto del proyecto.
- 2 puntos (Básico): Propuesta que cumple con los requisitos mínimos del pliego, sin aportar valor añadido o soluciones diferenciadoras.
- 0 puntos (Inadecuada): Propuesta sin contexto, insuficiente o fuera del alcance de los requisitos del pliego, con omisiones relevantes en la metodología o en la descripción de las soluciones propuestas. No demuestra adecuación a los objetivos del contrato ni ofrece garantías de ejecución efectiva.

2. Planificación del servicio (40 puntos)

Se evaluará la planificación temporal y operativa del servicio, con especial atención a su viabilidad y capacidad de adaptación. Se valorará:

- La estructura general del cronograma de trabajo, su claridad y coherencia con la duración del contrato.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

- La identificación de fases, hitos intermedios y entregables esperados en la ejecución del servicio.
- La existencia de un modelo de seguimiento y control del avance, con indicadores o puntos de verificación.
- La identificación de riesgos potenciales en la ejecución y la propuesta de medidas de contingencia y mitigación.
- La flexibilidad de la planificación para adaptarse a prioridades cambiantes o situaciones excepcionales en el entorno de auditoría o en las entidades auditadas.

Baremo de valoración:

- 10 puntos (Excelente): Cronograma perfectamente adecuado para el contexto, exhaustivo y bien estructurado, con mecanismos de seguimiento claros y medidas proactivas de gestión de riesgos y contingencias. Permite una visión integral y flexible, garantizando el control del proyecto en cada fase.
- 7 puntos (Muy bueno): Planificación bien definida y adecuada al contexto, aunque con detalles mejorables en ciertos hitos o mecanismos de control. Buena previsión de riesgos, aunque no completamente desarrollada en algunos escenarios.
- 5 puntos (Adecuado): Planificación básica y poco alineada con el alcance del proyecto, que cubre las fases principales, pero presenta carencias en la profundidad del análisis de riesgos y en la previsión de contingencias.
- 2 puntos (Básico): Planificación mínima, con escasa alineación al alcance, limitada a cumplir con los requisitos básicos del pliego, sin mecanismos claros de seguimiento ni previsión de riesgos adecuada.
- 0 puntos (Inadecuada): Planificación insuficiente, desestructurada o incompleta, sin cronograma definido ni previsión de riesgos. No garantiza el control efectivo del proyecto ni el cumplimiento de los hitos establecidos.

7.3. PRECIO DE LA OFERTA

40 puntos, valorable según la fórmula seleccionada:

(X) Función **optimizar precio**:

$$Ci = P * \frac{Ol - Oi}{Ol - Ob}$$

Donde:

Ci, es la puntuación en base al criterio precio, asignada a la oferta del licitador i

P, es la ponderación del criterio precio, la cual deberá ser como mínimo de 40 puntos sobre 100. El precio no puede ser el único criterio de adjudicación

Oi, es el precio ofertado por el licitador i (IVA excluido)

Ob, es el precio más bajo ofertado (IVA excluido)

Ol, es el presupuesto máximo de licitación (IVA excluido)

() Función **minimizar precio**:

$$Ci = P * \left(1 - \frac{Oi - Omin}{Omax} \right)$$



Donde:

C_i , es la puntuación en base al criterio precio, asignada a la oferta del licitador i

P , es la ponderación del criterio precio, la cual deberá ser como mínimo de 40 puntos sobre 100. El precio no puede ser el único criterio de adjudicación

O_i , es el precio ofertado por el licitador i (IVA excluido)

O_{min} , es el precio más bajo ofertado (IVA excluido)

O_{max} , es el precio de la oferta más alta (IVA excluido)

7.4. OTROS CRITERIOS AUTOMÁTICOS EVALUABLES MEDIANTE FÓRMULAS, DISTINTOS AL PRECIO

Criterios evaluables mediante fórmulas (**11%** del peso global)

CRITERIO	PONDERACIÓN EN PUNTOS (SOBRE 11)	FÓRMULA DE VALORACIÓN, según apartado 7.5.
Otros criterios automáticos evaluables mediante fórmulas:		
Plazo de puesta a disposición del equipo de proyecto una vez formalizada y comunicada la adjudicación (mínimo 5 días / máximo 20 días laborables)	6	Función <i>minimizar</i>
Número adicional de entidades beneficiarias del proceso completo de adecuación y certificación ENS (máximo admisible: 5 entidades adicionales)	5	Función <i>maximizar</i>

En coherencia con los criterios técnicos admisibles definidos en el Pliego del Acuerdo Marco SDA 26/2021, en este contrato específico se han seleccionado los siguientes criterios automáticos orientados a valorar la **eficacia operativa, la capacidad de respuesta y el alcance efectivo del servicio ofertado**, garantizando la objetividad y proporcionalidad en la puntuación.

- Plazo de puesta a disposición del equipo de proyecto (hasta 6 puntos). Se valorará la agilidad con que el adjudicatario pone a disposición el equipo de trabajo tras la formalización y comunicación de la adjudicación. El plazo se expresará en **días laborables**, contados desde el día siguiente a la comunicación formal de la adjudicación hasta la constitución efectiva y presentación del equipo y plan de trabajos.
 - Cualquier valor ofertado inferior a 5 se considerará igual al umbral mínimo (5 días).
 - Cualquier valor ofertado superior a 20 se considerará igual al umbral máximo (20 días).
 - No se admite una demora superior a 20 días laborables; cualquier valor excedente se ajustará al umbral máximo a efectos de valoración.
- Número adicional de entidades beneficiarias del proceso completo de adecuación y certificación ENS (hasta 5 puntos). Se valorará el compromiso del licitador de **ampliar el número solicitado expresamente en los requisitos (Anexo II) de entidades locales** (cinco ayuntamientos) que recibirán el proceso completo de adecuación y certificación ENS, respecto al mínimo obligatorio previsto en el contrato. La oferta indicará el número adicional propuesto, con un límite máximo de 5 entidades adicionales.



- Cualquier valor ofertado superior a 5 entidades se considerará igual al umbral máximo de 5.

7.5. FÓRMULAS APLICABLES A LOS CRITERIOS AUTOMÁTICOS EVALUABLES MEDIANTE FÓRMULAS

Función **Maximizar**:

$$C_i = P \cdot \frac{X_i}{X_{\max}}$$

Donde:

- C_i es la puntuación en base al criterio C, asignada a la oferta del licitador i;
- P es la ponderación del criterio C;
- X_i es el valor ofertado por el licitador i en el criterio C;
- X_{\max} es el valor máximo ofertado por los licitadores en el criterio C o el umbral de sociedad si éste fuese inferior y se hubiese definido.

En consecuencia, se asignarán P puntos a la oferta que presente mayor valor del dato en su oferta, en el criterio C, y al resto de ofertas se les asignarán las puntuaciones de forma lineal, según la fórmula anterior.

Función **Minimizar**:

$$C_i = P \cdot \left[1 - \left(\frac{X_i - X_{\min}}{X_{\max} - X_{\min}} \right) \right]$$

Donde:

- C_i es la puntuación en base al criterio C asignada a la oferta del licitador i;
- P es la ponderación del criterio C;
- X_i es el valor ofertado por el licitador i en el criterio C;
- X_{\min} es el valor mínimo ofertado por los licitadores en el criterio C o el valor mínimo de referencia que se hubiese definido, en su caso;
- X_{\max} es el valor máximo ofertado por los licitadores en el criterio C.

En consecuencia, se asignarán P puntos a la oferta que presente menor valor del dato en su oferta en el criterio C y al resto de ofertas se les asignarán las puntuaciones de forma lineal, según la fórmula anterior.

Función **Sí/No** (maximizar binario):

$$X_i = P$$

Donde:

- P es el peso del criterio a valorar, si la oferta del licitador contempla el cumplimiento de este requisito. En caso contrario, P es cero.

7.6. APLICACIÓN DEL UMBRAL DEL 50% DE PUNTUACIÓN

(**X**) El presente procedimiento se articula en dos fases correspondientes a la valoración de criterios sujetos a juicio de valor y la correspondiente a criterios evaluables mediante fórmulas (Sobres nº1 y Sobre nº 2). Conforme a lo previsto en el artículo 146.3 de la LCSP y en el apartado 27.5.4 del PCAP el límite del 50% de los criterios de calidad será aplicable una vez abierto el Sobre nº 1 (o si existiesen también criterios de calidad automáticos, una vez abierto el sobre 2.1 que contiene los valores de éstos).

() El presente procedimiento se articula en una única fase, al no existir criterios de adjudicación cuya cuantificación dependa de un juicio de valor.



8. OFERTAS ANORMALMENTE BAJAS

Se apreciará que la oferta es anormalmente baja conforme a lo señalado:

(**X**) Cuando se den las condiciones conforme a lo definido en la REGLA GENERAL

() Cuando se den las condiciones conforme a lo definido en la REGLA PARTICULAR

A. REGLA GENERAL DEL SISTEMA DINÁMICO

Cuando se produzcan las siguientes condiciones de forma concurrente:

- Si existiendo 4 o más licitadores las ofertas económicas presentadas resultan inferiores en más de 20 unidades porcentuales a la media aritmética de las ofertas presentadas. No obstante, si entre ellas existen ofertas que sean superiores a dicha media en más de 20 unidades porcentuales, se procederá al cálculo de una nueva media sólo con las ofertas que no se encuentren en el supuesto indicado. En todo caso, si el número de las restantes ofertas es inferior a tres, la nueva media se calculará sobre las tres ofertas de menor cuantía. Si, por el contrario, han concurrido menos de cuatro licitadores, resultarán de aplicación las previsiones del artículo 85 apartados 1 a 3 del Reglamento 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas.
- A la condición anteriores se deberá añadir la siguiente para apreciar el carácter anormal o desproporcionado de las ofertas.
 - () Cuando el criterio de calidad de mayor peso de los apartados 7.2 y 7.4 se encuentre fuera del umbral indicado:
 - (**X**) Cuando la puntuación de la totalidad de los criterios de calidad (todos los que no son el criterio precio) se encuentre fuera del umbral indicado: **30%**.

B. REGLA PARTICULAR

No aplica.

9. CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA

9.1. OBLIGACIONES GENERALES

Al presente contrato le resultan de aplicación las siguientes obligaciones, conforme a lo establecido en los pliegos reguladores del sistema dinámico de adquisición:

- a) Las obligaciones establecidas en el apartado 27.5.9 del PCAP respecto al personal laboral
- b) La obligación de confidencialidad del apartado 27.5.8 del PCAP
- c) Las obligaciones referidas a la protección de datos personales, en los términos previstos en la cláusula 27.5.7 apartado 2 del PCAP.
- d) La obligación de cumplimiento de la condición especial de ejecución relativa a la disponibilidad de los planes de formación conforme al apartado 27.5.7 apartado 1 del PCAP del SDA 26/2021 y, en su caso, las condiciones de ejecución previstas en el apartado 9.4. de este documento de invitación.



- e) Las obligaciones de comunicación de la subcontratación y la acreditación de los pagos a los subcontratistas conforme al apartado 27.11 del PCAP. En su caso, y conforme a lo previsto en el apartado 215.2.e):

(X) No existen tareas críticas que no puedan ser subcontratadas en el presente contrato específico.

() Las siguientes tareas críticas no podrán ser objeto de subcontratación, debido a las siguientes causas:

- No aplica.

- f) El cumplimiento de las condiciones salariales de los trabajadores conforme al convenio colectivo sectorial de aplicación conforme al artículo 122.2 de la LCSP.
- g) El adjudicatario nombrará un Coordinador Técnico del Contrato que actuará como interlocutor único a todos los efectos frente a la entidad destinataria del contrato, canalizando las comunicaciones y responsabilizándose de la gestión de los trabajos y de la gestión del personal adscrito por parte de la empresa adjudicataria.
- h) La obligación de disponibilidad de los medios técnicos conforme a lo previsto en el apartado 2 del PPT, según se indique en el presente documento de invitación.
- i) La obligación establecida en el apartado 5 del PPT.
- j) La obligación referente a la cesión de la propiedad intelectual de los trabajos de desarrollo conforme al 308.1 de la LCSP

9.2. RECURSOS A APORTAR AL SERVICIO

() No se define un equipo mínimo. El adjudicatario realizará la prestación a su riesgo y ventura con los medios personales y materiales que incluya en su propuesta si bien se facilita un equipo de trabajo orientativo.

(X) Se define un equipo mínimo en el apartado 9.2.1. que el adjudicatario deberá aportar para la prestación del servicio como **condición de ejecución del mismo**. El adjudicatario realizará la prestación a su riesgo y ventura con los medios personales mínimos descritos, pudiendo aumentarlos si lo estima conveniente.

() Se solicita la adscripción al contrato de perfiles profesionales. El adjudicatario deberá aportar el equipo mínimo del apartado 9.2.1. y acreditar la adscripción al contrato de los medios y personas, en número y cualificación, que se definen en el apartado 9.2.2.

En el apartado 9.2.2 de este documento se justifica de manera reforzada la obligación de adscripción, además de justificarse la necesidad de los perfiles profesionales requeridos.

9.2.1. DEFINICIÓN DEL EQUIPO MÍNIMO U ORIENTATIVO

El equipo de proyecto proporcionado por el adjudicatario para la prestación del servicio se adaptará a los perfiles siguientes:

Perfil	Funciones básicas a realizar
Jefe de Proyecto (Especialidad Seguridad)	Este profesional tendrá la responsabilidad de liderar el equipo de trabajo, asegurando la correcta planificación, ejecución y supervisión de las actividades encomendadas. Sus funciones deberán ser:



Perfil	Funciones básicas a realizar
	<ul style="list-style-type: none"> - 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.
Consultor (Especialidad Seguridad)	<p>Este profesional será responsable de las tareas de diseño de un SGSI para las entidades del entorno local de la Comunidad de Madrid, así como la adaptación al ENS de algunas de ellas, y a ofrecer soporte al modelo de gobernanza de ciberseguridad a través de las siguientes actividades:</p> <ul style="list-style-type: none"> - Dirigir y ejecutar actividades de adecuación al ENS en entidades del ámbito local, realizando diagnósticos de conformidad, análisis de riesgos, planes de acción y seguimiento del cumplimiento normativo. - Diseñar, implantar y mantener el modelo de gobernanza de ciberseguridad, definiendo roles, responsabilidades, políticas, procedimientos y métricas alineadas con marcos como ISO 27001, NIST y ENS, garantizando la integración con la estrategia institucional. - Asesorar en la gestión de riesgos y la protección de activos críticos, incluyendo sistemas municipales, datos de ciudadanos, padrón, asegurando la confidencialidad, integridad y disponibilidad de la información. - Prestar soporte a la Agencia en la toma de decisiones estratégicas, elaboración de documentación técnica y regulatoria, y coordinación con entidades de certificación.
Consultor (Cumplimiento Legal)	<p>Este profesional será responsable de prestar asesoramiento especialista al resto del equipo de trabajo y también de la propia Agencia en cumplimiento legal aplicable, con foco en el ENS. Las principales funciones deberán ser:</p> <ul style="list-style-type: none"> - Identificar brechas normativas y desarrollar propuestas de medidas correctivas para garantizar la conformidad con el ENS, NIS2 y RGPD. - Analizar y evaluar las políticas, normas y procedimientos internos de las entidades auditadas, alrededor de sus sistemas de información esenciales, asegurando su adecuación a los marcos legales y normativos aplicables.
Analista (Especialidad Seguridad)	<p>Este profesional tendrá un perfil similar al de Consultor (Especialidad Seguridad) en cuanto al desarrollo de sus funciones, aunque con menos experiencia y por tanto su labor será fundamentalmente de apoyo en tareas de trabajo de campo.</p>

En base a los anteriores perfiles, el equipo mínimo a aportar al proyecto es el siguiente:

Perfil	Número de personas	Dedicación
Jefe de Proyecto (Especialidad Seguridad)	1	50% / inicio contrato – fin contrato
Consultor (Especialidad Seguridad)	3	Completa / inicio contrato – fin contrato
Consultor (Cumplimiento Legal)	1	Completa / inicio contrato – fin contrato
Analista (Especialidad Seguridad)	3	Completa / inicio contrato – fin contrato



9.2.2. ADSCRIPCIÓN DE MEDIOS PERSONALES O MATERIALES

No aplica.

9.2.3. DOCUMENTACIÓN JUSTIFICATIVA DE DISPONER DE LOS MEDIOS A QUE SE HUBIESE COMPROMETIDO A DEDICAR O ADSCRIBIR AL CONTRATO

(☒) Los títulos oficiales que acrediten el cumplimiento de los requisitos de titulación exigida para los perfiles profesionales a dedicar al contrato.

(☒) La experiencia exigida para los perfiles profesionales, se acreditará mediante los currículum vitae detallados y anonimizados acompañados de declaración responsable del licitador sobre la veracidad de los datos contenidos en los mismos.

(☐) Aquella que acredite que los perfiles profesionales a adscribir a la ejecución del contrato pertenecen a la empresa, o que existe un precontrato para su incorporación laboral a la misma, o una relación mercantil que permita al empresario disponer de los mismos para la ejecución del contrato.

(☐) Otros

9.2.4. CONSTITUCIÓN DEL EQUIPO DE TRABAJO

El equipo de trabajo deberá estar constituido en el plazo de 15 días, a contar desde la fecha de notificación de la adjudicación del contrato específico.

9.2.5. RÉGIMEN DE SUSTITUCIÓN DEL PERSONAL

En el caso de que fuese necesaria la sustitución del personal adscrito, se deberá comunicar al responsable del contrato específico con la antelación suficiente y en todo caso en un plazo de quince días la sustitución propuesta para que pueda comprobarse que el nuevo componente que se pretende adscribir al contrato cumple las condiciones mínimas exigibles al perfil correspondiente.

9.3. ESQUEMA NACIONAL DE SEGURIDAD

Son condiciones de obligado cumplimiento las descritas en este documento, en el *Anexo VI Cumplimiento del Esquema Nacional de Seguridad*.

En aplicación del artículo 38 del ENS, el organismo destinatario:

(☐) Ha categorizado el sistema o sistemas objeto del desarrollo, de la siguiente manera: No aplica.

URL donde se publica la certificación o declaración de conformidad (art. 38.2 del ENS): *No aplica*.

(☒) No dispone todavía de la categorización del sistema o sistemas objeto del desarrollo.

En virtud de la anterior categorización, son de aplicación las medidas del Anexo II del ENS que se recogen en el Anexo VI de este documento. Para la aplicación de estas medidas se hace constar:



Medida Anexo VI	Aplicación
2.a. Mínimo privilegio	La Agencia dará las instrucciones.
2.b. Metodología desarrollo seguro	La Agencia dará las instrucciones.
2.c. Seguridad desde el diseño	La Agencia dará las instrucciones.

Adicionalmente a lo anterior y de conformidad con el artículo 14 del ENS, el organismo destinatario ha realizado un análisis previo de riesgos a los que está expuesto el sistema, empleando una metodología reconocida internacionalmente. A resultados de dicho análisis, el responsable del servicio ha determinado los siguientes requisitos aplicables al servicio de desarrollo prestado, adicionales a todos los anteriores:

☒ (X) No se han determinado requisitos aplicables al servicio de desarrollo del sistema.

☐ () Se han determinado los siguientes requisitos aplicables al servicio de desarrollo del sistema: No aplica.

9.4. OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO

No aplica.

10. PAGO DE LOS SERVICIOS Y FACTURACIÓN

El pago de los trabajos efectivamente realizados de conformidad con los términos del contrato se efectuará de acuerdo con lo establecido en los artículos 198 y 199 de la LCSP y las normas y disposiciones que los desarrollan.

La **periodicidad de los pagos** será la siguiente:

☐ () **Mensual** para los trabajos descritos incluidos en

- ☐ () ANEXO II
- ☐ () ANEXO III
- ☐ () ANEXO IV

☐ () **Trimestral**, para los trabajos según los trabajos descritos incluidos en

- ☐ () ANEXO II
- ☐ () ANEXO III
- ☐ () ANEXO IV

considerando los siguientes períodos trimestrales: No aplica.

☒ (X) Conforme a los hitos establecidos en el ANEXO II al recibirse los entregables.

- ☒ (X) Los hitos tienen naturaleza de entregas parciales
- ☐ () Los hitos se abonan como anticipos a cuenta, debido a la naturaleza de la prestación

☐ () Otra



La cuantía a pagar por la Administración será el importe ofertado por el adjudicatario correspondiente a los trabajos completados que haya desempeñado el contratista en el período de facturación.

10.1. CONDICIONES DE PRESENTACIÓN DE LAS FACTURAS

() Organismo incluido en el ámbito subjetivo, art 229.2 LCSP.

Las facturas se presentarán obligatoriamente en formato electrónico firmadas con firma electrónica avanzada basada en un certificado reconocido. En concreto, las facturas electrónicas que se remitan a las Administraciones Públicas se ajustarán al formato estructurado de la factura electrónica Facturae y de firma electrónica conforme a la especificación XMLAdvanced Electronic Signatures (XAdES).

En las facturas deberán constar los siguientes datos, de conformidad con lo dispuesto en la disposición adicional trigésima segunda de la LCSP:

- Órgano de contratación: Dirección General de Racionalización y Centralización de la Contratación - E04962703.
- Órgano responsable del contrato específico: No aplica.
- Órgano gestor: No aplica.
- Unidad tramitadora: No aplica.
- Órgano administrativo con competencias en materia de contabilidad pública: No aplica.

Asimismo, en el ámbito de la facturación electrónica deberán incluir:

- Campo <FileReference>: SDA 26/2021.
- Campo <Receiver transaction reference>: Será el número del contrato específico (xxxx/aaaa) o, en su defecto, el número que para esta tramitación asigne el organismo destinatario.

(X) Organismo adherido al Sistema Estatal de Contratación Centralizada.

La Agencia de Ciberseguridad de la Comunidad de Madrid gestionará, con un procedimiento automatizado, las facturas recibidas en el “Punto General de Entrada de Facturas Electrónicas”, FACE, en los términos establecidos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y sus disposiciones de desarrollo.

En las facturas deberán constar los siguientes datos, de conformidad con lo dispuesto en la disposición adicional trigésima segunda de la LCSP:

- Órgano de contratación: Agencia de Ciberseguridad de la Comunidad de Madrid – Q2802867H.
- Código DIR3: El código único para el órgano gestor, la unidad tramitadora y la oficina contable es el A13050393.

Asimismo, en el formato electrónico de la factura se debe incluir el número de pedido asignado por la Agencia en el campo ReceiverTransactionReference.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

El pago de los servicios se efectuará por el organismo destinatario, según lo previsto en las normas que regulen el procedimiento para el pago de sus obligaciones.

En caso de ser de aplicación los preceptos indicados en el apartado anterior, deberán copiarse y consignarse aquí. En caso de que exista normativa específica, deberá incluirse aquí.

11. PLAZO DE GARANTÍA DEL OBJETO DEL SERVICIO

Una vez efectuada la recepción o conformidad según lo establecido en los artículos 210 y 311 de la LCSP, comenzará el plazo de garantía de los entregables que hacen objeto del contrato específico. Este plazo se fija en **nueve meses** desde la fecha de recepción.

Si durante el plazo de garantía se acreditase la existencia de vicios o defectos en los entregables de la prestación contratada, el órgano de contratación tendrá derecho a reclamar al contratista la subsanación de los mismos en un plazo no superior a tres meses. Estos vicios y defectos se entenderán siempre referidos a la última versión del entregable generada por el contratista, no estando cubierta por esta garantía ninguna versión posterior de dicho entregable.

El contratista tendrá derecho a conocer y ser oído sobre las observaciones que se formulen en relación con el cumplimiento de la prestación contratada.

Terminado el plazo de garantía sin que la Administración haya formalizado ningún reparo o denuncia, el contratista quedará exento de responsabilidad por razón de la prestación efectuada.

12. PENALIDADES

12.1. PENALIDADES FIJADAS EN EL SISTEMA DINÁMICO DE ADQUISICIÓN

No aplica (el proyecto no reviste necesidades especiales, con agravantes sobre las penalidades definidas en los pliegos del SDA26).

12.2. FÓRMULA PARA LA APLICACIÓN DE PENALIDADES

Los porcentajes para los incumplimientos que no deban calificarse como graves o muy graves, se aplican sobre el importe de la facturación del período en el que se produzca el incumplimiento que da lugar a la penalidad, mediante la siguiente fórmula:

$$I_P = 0.01 \times I_F \frac{d}{D}$$

Donde:

- I_P es el importe de la penalidad a aplicar
- I_F es el importe del periodo de facturación, antes de la aplicación de ninguna penalidad
- d es el número de días hábiles durante los que ha subsistido el incumplimiento dentro del periodo de facturación, y
- D es el número de días hábiles contenidos en el periodo de facturación.

13. CAUSAS DE RESOLUCIÓN DE LOS CONTRATOS ESPECÍFICOS



No aplica (el proyecto no reviste necesidades especiales, con causas de resolución adicionales a las previstas en los pliegos del SDA26).

14. FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS

Las ofertas se presentarán obligatoriamente en formato electrónico, a través de la PLACSP² u otra plataforma de contratación a disposición del organismo.

Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa³.

El organismo destinatario deberá realizar el trámite de apertura de las ofertas siguiendo los preceptos de la licitación electrónica.

Las ofertas contendrán como mínimo la siguiente información:

- **Sobre 1: Documentación relativa a los criterios de adjudicación cuya ponderación está sujeta a un juicio de valor.**

La oferta técnica no podrá contener información ni dato alguno relacionado con los criterios de valoración mediante fórmula, advirtiéndose de que, en otro caso, la oferta podrá ser excluida. La oferta técnica no deberá contener:

- Información ni documentación adicional relativa a la presentación de la empresa.
- Referencias de otros proyectos realizados.
- Otras cuestiones de tipo general sin relación concreta con el objeto del contrato.
- Información detallada sobre el dimensionamiento y características del equipo de trabajo. Estos datos se aportarán, en su caso, en el Sobre nº 2.1.

Los documentos que se incluyen en este sobre son los siguientes:

- **Documento Único OFERTA TÉCNICA** Elaboración del Documento de Oferta Técnica cuya extensión no deberá exceder las **22 páginas** en formato DIN A4 a doble cara cada hoja, con un tamaño de letra mínimo de 10 puntos e interlineado sencillo. Toda oferta técnica que incumpla las características anteriores y que no incluya las descripciones técnicas que sean necesarias para que se pueda valorar la adecuación de la oferta al cumplimiento del objeto del contrato, no será objeto de valoración (Resolución nº 985/2015 del TRIBUNAL ADMINISTRATIVO CENTRAL DE RECURSOS CONTRACTUALES).
- **Sobre 2**
 - **2.1: Documentación relativa a los criterios automáticos evaluables mediante fórmulas, distintos del precio.** Se recomienda presentar esta documentación utilizando la siguiente tabla:

² Plataforma de Contratación del Sector Público:
<https://contrataciondelestado.es/wps/portal/quiasAyuda>

³ Para facilitar la identificación del firmante apoderado de la empresa, se deberá indicar, además de sus datos, el número de usuario apoderado de la aplicación CONECTA-CENTRALIZACIÓN.

Criterios automáticos evaluables mediante fórmula, distintos del precio	
Plazo de puesta a disposición del equipo de proyecto una vez formalizada y comunicada la adjudicación (mínimo 5 días / máximo 20 días laborables)	Valor (entre 5 y 10)
Número adicional de entidades beneficiarias del proceso completo de adecuación y certificación ENS (máximo admisible: 5 entidades adicionales)	Valor (hasta 5)

○ **2.2: Oferta económica**

La oferta incluirá, en todo caso, la **propuesta económica global** para la ejecución del contrato conforme a los hitos y entregables definidos en el Anexo II.3 (HITO_01 a HITO_04). Esta propuesta incluirá el importe total, desglosando como partida independiente el IVA correspondiente. Se recomienda presentar esta documentación utilizando la siguiente tabla:

Criterio precio	
Base Imponible:	€
21 % IVA:	€
Importe total, IVA incluido:	€

Las ofertas firmadas electrónicamente se presentarán a través de la Plataforma para la Contratación de la Comunidad de Madrid, y según sus normas:

<https://contratos-publicos.comunidad.madrid/>

Para consultas se habilita un plazo que será, desde el día siguiente de la recepción de la invitación a participar en la licitación, hasta 7 días naturales antes de la fecha de finalización del plazo de presentación de ofertas.

Las consultas se remitirán por correo electrónico a la siguiente dirección de correo electrónico: Licita_Agencia_Ciber@madrid.org.

Con la finalidad de dar cumplimiento a las medidas destinadas a las entidades adheridas para velar por la correcta aplicación de los términos, condiciones e instrucciones que regulan el Sistema Dinámico de Adquisición de Servicios de desarrollo de sistemas de administración electrónica (SDA 26/2021), los pliegos rectores del SDA se encuentran disponibles en el siguiente enlace:

https://contratacioncentralizada.gob.es/ficha-sda/-/journal_content/XXA1X8YVROqE?_56_INSTANCE_XXA1X8YVROqE_articleId=194658&_56_INSTANCE_XXA1X8YVROqE_groupId=11614



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

NOTAS IMPORTANTES: NO ES NECESARIO COMUNICAR QUE NO SE VA A CONCURRIR A LA LICITACIÓN AL NO REQUERIR OBLIGATORIAMENTE LA PRESENTACIÓN DE OFERTAS EL PRESENTE SISTEMA DINÁMICO.

EN LO QUE ESTE DOCUMENTO DE INVITACIÓN SE OPONGA A LOS PLIEGOS DEL SISTEMA DINÁMICO DE ADQUISICIÓN, PREVALECEERÁN ESTOS ÚLTIMOS.

NO ES VÁLIDO INTRODUCIR EL CONTENIDO DE LOS APARTADOS 1 A 14 DE ESTA INVITACIÓN EN LOS ANEXOS U OTROS ESPACIOS DIFERENTES A LOS PREVISTOS EN ESTE MODELO PARA CONTENER ESA INFORMACIÓN

EL TITULAR DEL ÓRGANO DESTINATARIO: *(El Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid.*

Firmado electrónicamente: *D. Alejandro Las Heras Vázquez*

Firmado digitalmente por: LAS HERAS VÁZQUEZ ALEJANDRO
Fecha: 2026.02.06 11:42



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA

A. OBLIGACIONES GENERALES APLICABLES A TODOS LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA

En todos los contratos basados financiados⁴ por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiables, estableciéndose las siguientes **obligaciones**:

1. ADECUACIÓN DEL CONTRATO A LAS PREVISIONES ESPECÍFICAS DEL INSTRUMENTO DE PLANIFICACIÓN ESTRATÉGICA

El contrato deberá cumplir las condiciones previstas en el instrumento de programación del acuerdo /programa marco/ programa operativo/eje/criterio para el que resulte seleccionado para apoyo por los fondos o programas.

Específicamente en los contratos financiados con cargo al PRTR deberán cumplirse las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control en el componente/inversión.

2. PRINCIPIO DO NO SIGNIFICANT HARM (“DNSH”)

La ejecución del contrato está sujeta a los objetivos medioambientales del artículo 17 del Reglamento UE nº 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020, relativo al establecimiento de un marco para facilitar las inversiones sostenibles, y en concreto a las condiciones del componente/inversión del PRTR.

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

Al presente contrato le resulta de aplicación el Plan de medidas antifraude y anticorrupción, con el contenido mínimo establecido en los sistemas de gestión de las autoridades de los Fondos, Mecanismos o Programas Europeos. En el caso de los contratos del PRTR le será de aplicación lo previsto en la Orden HFP/1030/2021, de 29 de septiembre y el Plan aprobado por el organismo destinatario de la prestación.

4. AUSENCIA DE CONFLICTO DE INTERESES

Al presente contrato le resultan de aplicación las normas que garantizan la prevención de los conflictos de interés, conforme al considerando 104 y al artículo 61 del Reglamento Financiero de la UE, debiendo adoptarse las debidas precauciones durante todas las fases de tramitación y ejecución de los mismos.

En particular, no se considerarán admisibles los intentos de influir indebidamente en el presente procedimiento de adjudicación u obtener información confidencial.

Los participantes en el procedimiento deben cumplimentar la declaración de ausencia de conflicto de interés (DACI) en los términos previstos en los planes de medidas antifraude y anticorrupción. En los contratos sujetos al PRTR, las medidas serán conformes con las disposiciones de la Orden HFP/1030/2021.

⁴ O es susceptible de ser financiado en caso de no haberse aún confirmado la selección por las autoridades correspondientes.



5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

El contrato está sujeto a cuantas medidas de información, comunicación y visibilidad sean requeridas por la normativa que comunitaria y en particular, las medidas que resulten de obligado cumplimiento para las actuaciones y proyectos financiados con cargo al (Instrumento de Recuperación de la UE/Fondo/Programa xxx).

6. ACEPTACIÓN DE LOS PRINCIPIOS DE BUENA GESTIÓN FINANCIERA Y SOMETIMIENTO A CONTROLES DE LAS AUTORIDADES PREVISTAS EN LOS FONDOS O MECANISMOS

Todas las actuaciones contractuales deben observar los principios de buena gestión financiera.

El contrato está sujeto a las actuaciones de control que sean de aplicación a las ayudas conforme a la normativa comunitaria, que podrán ser efectuadas por la Comisión Europea, la Oficina de Lucha contra el Fraude (OLAF), el Tribunal de Cuentas Europeo, la Fiscalía Europea, así como a las autoridades nacionales designadas para la gestión o control de los fondos, programas o mecanismos, a los que no podrá denegarse el acceso a la información del contrato.

7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

Los beneficiarios deberán conservar la información del expediente de contratación conforme a lo dispuesto en el artículo 132 del Reglamento Financiero de la UE, u otros plazos de disponibilidad que puedan establecerse en los reglamentos comunitarios de los fondos/programas o mecanismos.

En el caso de los contratos financiados en el PRTR los organismos destinatarios se asegurarán de dejar constancia en el expediente de contratación de las actuaciones que acreditan los principios de gestión específicos del Plan, conforme a las recomendaciones contenidas en la Instrucción de la Junta Consultiva de Contratación Pública de 23 de diciembre sobre aspectos a incorporar en los expedientes que se vayan a financiar con fondos procedentes del PRTR.

8. PROHIBICIÓN DE DOBLE FINANCIACIÓN

Conforme al considerando 130 y al artículo 191.3 del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo de 18 de julio de 2018 (Reglamento Financiero de la UE), en ningún caso podrán ser financiados dos veces por el presupuesto de la Unión Europea los mismos gastos.

B. OBLIGACIONES GENERALES APLICABLES A LOS CONTRATOS FINANCIADOS CON CARGO AL PRTR

1. RÉGIMEN JURÍDICO APLICABLE

El contrato, al estar incluido en el PRTR, está sometido al Real Decreto-ley 36/2020, de 30 de diciembre, a la Orden HFP/1030/2021, de 29 de septiembre, a la Orden HFP/1031/2021, de 29 de septiembre, y a cuantas normas de desarrollo se aprueben.

La financiación del contrato se efectúa con cargo a fondos del Mecanismo de Recuperación y Resiliencia de la Unión Europea – Next Generation EU- establecido por el Reglamento (UE) 2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, y



regulado según el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.

2. COMPONENTE E INVERSIÓN Y COMPROMISOS ASUMIDOS POR LA CONTRIBUCIÓN AL ETIQUETADO VERDE Y DIGITAL Y POR EL PRINCIPIO DE NO CAUSAR DAÑO SIGNIFICATIVO AL MEDIOAMBIENTE (DNSH)

El contrato se enmarca en el **Componente C15. Inversión I07**

“Ciberseguridad: Fortalecimiento de las capacidades de Ciberseguridad de ciudadanos, PYMES y profesionales; impulso del ecosistema del sector”

Conforme al PRTR aprobado esta inversión contribuye en materia de etiquetado verde y digital en los siguientes porcentajes.

Etiquetado verde	Etiquetado digital
0%	100%

El PRTR incorpora las obligaciones específicas para la inversión en el Componente/Inversión que deberán cumplirse en la ejecución del presente contrato:

- Obligaciones del componente/inversión por el **etiquetado verde**: No existen obligaciones específicas para este componente e inversión.
- Obligaciones al componente/inversión por el **etiquetado digital**: El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, establece en sus Anexos VI y VII la Metodología de seguimiento para la acción por el clima y la metodología para el etiquetado digital en el marco del Mecanismo, respectivamente. Según estos anexos, el Campo de Intervención 021quinquies – Desarrollo y despliegue de tecnologías, medidas e instalaciones de apoyo en materia de ciberseguridad para los usuarios de los sectores público y privado, contribuye con un 0% al cálculo de la ayuda de los objetivos climáticos y medioambientales, y con un 100% al cálculo de la ayuda a la transición digital. El presente contrato tiene por objeto la prestación de un servicio de consultoría técnica especializada, y esta actuación se enmarca en el Componente C15 del Plan de Recuperación, transformación y Resiliencia (PRTR). Orientado a la mejora de la conectividad digital, el impulso de la ciberseguridad y la transformación digital de las administraciones públicas. La naturaleza del contrato permite justificar una contribución del 100% al etiquetado digital, conforme a los criterios establecidos por la Comisión Europea y la normativa nacional aplicable
- Condiciones que deben cumplir las prestaciones establecidas en la evaluación de los aspectos del principio de DNSH (*Do No Significant Harm*) con relación los seis objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020. No aplica.

3.- CLÁUSULA DE MODIFICACIÓN DE LOS CONTRATOS BASADOS FINANCIADOS EN EL PRTR

Sin perjuicio de las causas de modificación previstas en el documento de licitación, en caso de estar financiado el presente contrato basado/específico con cargo al PRTR, podrá ser modificado, si la Autoridad Responsable del mecanismo ordena la adopción de medidas



correctoras por haberse evidenciado deficiencias durante la ejecución del contrato que afectan a alguno de los objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020 que pueden causar un daño significativo al medioambiente.

4.- PENALIDADES POR EJECUCIÓN DEFECTUOSA O INCORRECTA EJECUCIÓN DE LOS CONTRATOS BASADOS FINANCIADOS EN EL PRTR

En caso de incumplimiento o cumplimiento defectuoso por el contratista de los compromisos adquiridos en base a las obligaciones establecidas en este documento de licitación en relación al PRTR, se podrán imponer al contratista las siguientes penalidades conforme a lo previsto en los artículos 192 a 195 de la LCSP:

☒ (X) No aplica

☐ () Por incumplimiento de las obligaciones establecidas para los productos en el etiquetado verde o etiquetado digital.

☐ () Por falta de acreditación a requerimiento del responsable del contrato en el plazo de 10 días hábiles.

☐ () Por incumplimiento.

☐ () Por incumplimiento de las obligaciones asociadas al DNSH del componente/inversión:

☐ () Otras penalidades

5.- OBLIGACIONES DE ACREDITACIÓN PARA LOS LICITADORES, CONTRATISTAS Y SUBCONTRATISTAS ESTABLECIDAS EN EL PRTR

En el marco de la protección de los intereses financieros de la Unión Europea, y en concreto del Artículo 22 del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, la Comisión Europea requiere la identificación de los titulares reales de las entidades contratistas o beneficiarias del Plan de Recuperación, Transformación y Resiliencia, tal y como se define en el artículo 3 punto 6 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo.

Por ello, en base a lo establecido en el artículo 7 de la Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia, en caso de que no existan datos de titularidad real en las bases de datos de la AEAT de **un participante en el procedimiento de contratación**, el órgano de contratación solicitará a éste la información de su titularidad real. Esta información deberá aportarse al órgano de contratación en el plazo de cinco días hábiles desde que se formule la solicitud de información. La falta de entrega de dicha información en el plazo señalado será motivo de **exclusión** del procedimiento.

Los contratistas y, en su caso, subcontratistas están obligados específicamente a cumplir lo previsto en el sistema de gestión del Plan de Recuperación Transformación y Resiliencia, y en lo que les resulta de aplicación, se obligan a lo previsto la adenda. Adicionalmente deberán facilitar los siguientes datos de identificación:

- a) NIF del contratista y, en su caso de los subcontratistas
- b) Nombre o Razón Social



- c) Domicilio fiscal del contratista y, en su caso, subcontratistas
- d) Aceptación de la cesión de datos entre las Administraciones Públicas implicadas para dar cumplimiento a lo previsto en la normativa europea que es de aplicación y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (Modelo Anexo IV.B de la Orden HFP/1030/2021, de 29 de septiembre)
- e) Declaración responsable relativa al compromiso de cumplimiento de los principios transversales establecidos en el PRTR y que pudieran afectar al ámbito objeto de la gestión (Modelo Anexo IV.C de la Orden HFP/1030/2021, de 29 de septiembre)
- f) Los contratistas acreditarán la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT o en el Censo equivalente de la Administración Tributaria Foral, que debe reflejar la actividad efectivamente desarrollada en la fecha de participación en el procedimiento de licitación.

El propuesto como mejor clasificado, de forma previa a elevar la propuesta de adjudicación, deberá cumplimentar la DECLARACIÓN MULTIPLE en el formato previsto en el apartado B.6 de esta Adenda, relativa a contratos basados financiados con cargo al Plan de Recuperación, Transformación y Resiliencia (PRTR).

6. DECLARACIÓN MULTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS BASADOS FINANCIADOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

Don/Doña, DNI, como
Consejero Delegado/Gerente/ de la entidad.....,
con NIF, y domicilio fiscal en que participa
como contratista/subcontratista en el desarrollo de actuaciones necesarias para la consecución
de los objetivos definidos en el Componente XX «.....».

Efectúa las siguientes **DECLARACIONES**

a) Declaración relativa a la obligación de cesión y tratamiento de datos en relación con la ejecución de actuaciones del plan de recuperación, transformación y resiliencia (Modelo Anexo IV.B de la Orden HFP/1030/2021, de 29 de septiembre)

Que conoce la normativa que es de aplicación, en particular los siguientes apartados del artículo 22, del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, que se define a continuación:

1. La letra d) del apartado 2: «recabar, a efectos de auditoría y control del uso de fondos en relación con las medidas destinadas a la ejecución de reformas y proyectos de inversión en el marco del plan de recuperación y resiliencia, en un formato electrónico que permita realizar búsquedas y en una base de datos única, las categorías armonizadas de datos siguientes:

- i. El nombre del perceptor final de los fondos;
- ii. el nombre del contratista y del subcontratista, cuando el perceptor final de los fondos sea un poder adjudicador de conformidad con el Derecho de la Unión o nacional en materia de contratación pública;
- iii. los nombres, apellidos y fechas de nacimiento de los titulares reales del perceptor de los fondos o del contratista, según se define en el artículo 3, punto 6, de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo (26);



iv. una lista de medidas para la ejecución de reformas y proyectos de inversión en el marco del plan de recuperación y resiliencia, junto con el importe total de la financiación pública de dichas medidas y que indique la cuantía de los fondos desembolsados en el marco del Mecanismo y de otros fondos de la Unión».

2. Apartado 3: «Los datos personales mencionados en el apartado 2, letra d), del presente artículo solo serán tratados por los Estados miembros y por la Comisión a los efectos y duración de la correspondiente auditoría de la aprobación de la gestión presupuestaria y de los procedimientos de control relacionados con la utilización de los fondos relacionados con la aplicación de los acuerdos a que se refieren los artículos 15, apartado 2, y 23, apartado 1. En el marco del procedimiento de aprobación de la gestión de la Comisión, de conformidad con el artículo 319 del TFUE, el Mecanismo estará sujeto a la presentación de informes en el marco de la información financiera y de rendición de cuentas integrada a que se refiere el artículo 247 del Reglamento Financiero y, en particular, por separado, en el informe anual de gestión y rendimiento».

Que, conforme al marco jurídico expuesto, manifiesta **acceder a la cesión y tratamiento de los datos** con los fines expresamente relacionados en los artículos citados.

b) Declaración de compromiso en relación con la ejecución de actuaciones del plan de recuperación, transformación y resiliencia (PRTR) (Modelo Anexo IV.C de la Orden HFP/1030/2021, de 29 de septiembre)

Manifiesta el compromiso de la persona/entidad que representa con los estándares más exigentes en relación con el cumplimiento de las normas jurídicas, éticas y morales, adoptando las medidas necesarias para prevenir y detectar el fraude, la corrupción y los conflictos de interés, comunicando en su caso a las autoridades que proceda los incumplimientos observados.

Adicionalmente, atendiendo al contenido del PRTR, se compromete a respetar los principios de economía circular y evitar impactos negativos significativos en el medio ambiente («DNSH» por sus siglas en inglés «*do no significant harm*») en la ejecución de las actuaciones llevadas a cabo en el marco de dicho Plan, y manifiesta que no incurre en doble financiación y que, en su caso, no le consta riesgo de incompatibilidad con el régimen de ayudas de Estado.

c) Conforme a las obligaciones de aportación de información del apartado 5 de esta adenda

Acredita la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT (declaración censal 036 o 037⁵ o documento equivalente de las Administraciones Forales) que incluye la actividad objeto del contrato basado conforme a lo previsto en el artículo 8 apartado 2 de la Orden HFP/1030/2021, de 29 de septiembre).

d) Sin perjuicio de lo previsto en el artículo 215 de la LCSP, y con referencia a las obligaciones de los subcontratistas declara:

() Que **no** se presenta declaración en los términos del apartado 5 de esta adenda al documento de licitación correspondientes a otras empresas al no estar previsto acudir a la subcontratación.

() Que aporta las declaraciones de las siguientes empresas que actuarán como subcontratistas en el presente contrato:

⁵ Estas declaraciones podrán obtenerse por las empresas en la sede de la AEAT en el siguiente enlace <https://sede.agenciatributaria.gob.es/Sede/tramitacion/G322.shtml> . Si tienen dudas llamen al teléfono general de consultas de la Agencia Tributaria o al 060.



(Indicar CIF Y RAZON SOCIAL DE LAS EMPRESA SUBCONTRATISTAS de las que se aporta en documento adicional declaración firmada por sus representantes legales en el formato de este anexo)

....., XX de de 202X

Fdo.

Cargo:



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

ANEXO I DESCRIPCIÓN DEL ENTORNO TÉCNICO Y FUNCIONAL EXISTENTE

I.1. DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN EXISTENTES

No aplica.

I.2. DESCRIPCIÓN DEL ENTORNO TECNOLÓGICO

No aplica.

ANEXO II DEFINICIÓN Y ALCANCE DE LOS TRABAJOS

Contexto estratégico y marco del proyecto RESEDA

El presente contrato se enmarca en el Proyecto RESEDA (Resiliencia de los Datos en el Sector Público Local), una iniciativa estratégica incluida en el Plan de Recuperación, Transformación y Resiliencia (PRTR) del Gobierno de España, financiada a través del Mecanismo de Recuperación y Resiliencia de la Unión Europea (NextGenerationEU).

Las actuaciones contempladas en este contrato corresponden a la Línea 4 del Proyecto RESEDA, orientada a obtener un programa de refuerzo de la estrategia regional de ciberseguridad. Esta línea contribuye al cumplimiento de los objetivos del Componente 15, Inversión 7 del PRTR, centrados en reforzar las capacidades de ciberseguridad en los servicios públicos esenciales para la ciudadanía.

El sector local, debido a su criticidad, interdependencias y la sensibilidad de los datos que gestiona, se enfrenta a un entorno creciente de amenazas cibernéticas que ponen en riesgo tanto la seguridad de la información municipal como la continuidad de los servicios públicos. Ante este escenario, la Agencia de Ciberseguridad de la Comunidad de Madrid, creada mediante la Ley 14/2023, lidera la ejecución de actuaciones dirigidas a mejorar la ciberresiliencia del sector público local, impulsando un modelo regional coordinado y sostenible de gestión de la seguridad, soportado en una solución tecnológica multientidad y en mecanismos reforzados de gobernanza, comités y coordinación intermunicipal.

El marco legal y estratégico que sustenta este proyecto incluye el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), la Directiva (UE) 2022/2555 (NIS2) y la Directiva (UE) 2022/2557 (CER), así como el Esquema Nacional de Seguridad.

Asimismo, se reconoce que la madurez organizativa y tecnológica debe ir acompañada de mecanismos de gobernanza federada, incluyendo la dinamización de comités locales y el reforzamiento del Comité de Seguridad de la Información de la Comunidad de Madrid mediante la integración de los ayuntamientos. En este sentido, se pretende desarrollar un Sistema de Gestión de la Seguridad de la Información (SGSI) de la Agencia que englobe y coordine los SGSIs de las distintas entidades de la región, permitiendo así alinear los esfuerzos locales con la estrategia regional y facilitar una supervisión transversal del cumplimiento, la eficacia de los controles y la evolución de los riesgos.

Naturaleza del servicio y adecuación al entorno local

El presente contrato tiene carácter integral y especializado, orientado a contar con un modelo de SGSI efectivo y a la adaptación al Esquema Nacional de Seguridad en el ámbito de los



ayuntamientos de menos de 20.000 habitantes de la Comunidad de Madrid, así como a los principios de gobernanza federada, visibilidad ejecutiva del riesgo y mejora continua. Asimismo, el alcance del contrato se extiende a aquellos ayuntamientos de más de 20.000 habitantes que suscriban convenio o contrato con la Comunidad de Madrid para la ejecución de estos trabajos, garantizando así una cobertura homogénea y coordinada en materia de seguridad de la información en el sector público local.

El servicio combina componentes de:

- consultoría estratégica en materia de SGSI,
- soporte a la certificación (incluida la ejecución de auditoría externa), y
- fortalecimiento de los mecanismos de gobernanza y coordinación sectorial,

lo que exige un enfoque metodológico riguroso, una alta especialización en materia de ciberseguridad y una ejecución coordinada con múltiples entidades municipales.

La adecuación al sector local es un elemento central del contrato. Los ayuntamientos presentan una elevada exposición a riesgos digitales, gestionan información especialmente protegida, operan con infraestructuras críticas y se estructuran en organizaciones con alta diversidad funcional y tecnológica. Además, el alto grado de desconocimiento de la materia en entidades municipales y la escasez de talento en el sector, implica que el riesgo debe gestionarse de forma agregada y coordinada a nivel regional. La necesidad de asegurar la continuidad de los servicios públicos, garantizar la confidencialidad de los datos de ciudadanos y cumplir con un marco normativo exigente (ENS, RGPD, NIS2) hace imprescindible un modelo homogéneo y escalable de gestión de la seguridad.

El enfoque del servicio parte de la premisa de que el éxito en la implantación del ENS en el entorno local requiere:

- Una arquitectura común de gestión de la seguridad, que respete la autonomía municipal, pero garantice la coherencia regional, y la integración con la gestión de la Agencia de Ciberseguridad.
- Una metodología replicable y sostenible, que facilite el avance coordinado de los ayuntamientos hacia niveles adecuados de madurez en seguridad.
- Un modelo de gobernanza federado, que permita la supervisión colaborativa, la consolidación regional del riesgo y la coordinación reforzada a través del Comité de Seguridad de la Información y sus grupos sectoriales.
- El soporte a las necesarias auditorías externas, garantizando la obtención efectiva del certificado ENS en los ayuntamientos seleccionados.

Por tanto, el contrato se configura como un instrumento clave para avanzar hacia un sector público local más ciberresiliente, alineado con los principios de eficiencia, trazabilidad, responsabilidad institucional, integración sectorial, y protección efectiva de los derechos digitales de la ciudadanía.

Objeto y alcance del contrato

El presente contrato tiene por objeto la prestación de un servicio integral para el diseño e implantación de un modelo común de gestión de la seguridad de la información (SGSI) y de cumplimiento con el ENS para el entorno de los ayuntamientos de menos de 20.000 habitantes de la Comunidad de Madrid, y en el marco del Proyecto RESEDA. Sin menoscabo de aquellos ayuntamientos de más de 20.000 habitantes que suscriban un convenio o contrato con la Agencia de Ciberseguridad.



Asimismo, es importante señalar que, de acuerdo con lo establecido en la Ley 7/2022, de 8 de febrero, de creación de la Agencia de Ciberseguridad de la Comunidad de Madrid, publicada en el Boletín Oficial de la Comunidad de Madrid (BOCM) núm. 34, de 10 de febrero de 2022, los ayuntamientos de más de 20.000 habitantes están obligados a suscribir un convenio o contrato de colaboración con la Agencia de Ciberseguridad para la prestación de servicios en materia de seguridad de la información. En concreto, el artículo 8, apartado 3, de dicha ley establece: “Los municipios de la Comunidad de Madrid con una población superior a 20.000 habitantes deberán suscribir un convenio o contrato con la Agencia de Ciberseguridad para la prestación de los servicios de apoyo en materia de ciberseguridad”. Esta disposición refuerza la necesidad de coordinación y cumplimiento normativo en todos los ayuntamientos de la región, independientemente de su tamaño.

El servicio se prestará sobre un alcance funcional de los 144 ayuntamientos de menos de 20.000 habitantes, y la propia Agencia de Ciberseguridad de la Comunidad. En la Comunidad de Madrid hay un total de 179 ayuntamientos, que corresponden a los distintos municipios que conforman la región.

Todas las entidades serán destinatarias de los bloques de trabajo de planificación y definición de sistemas de gestión de la seguridad de la información comunes, y 5 de ellas serán seleccionadas para recibir el acompañamiento técnico para el proceso de auditoría externa de certificación ENS.

Este modelo de servicio se articula sobre los siguientes ejes operativos:

- Definición del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) de la propia Agencia
- Análisis del estado de situación de las entidades locales en materia de SGSI. Y asesoramiento para la selección de las 5 entidades donde vamos a reforzar el cumplimiento de la normativa en materia de ciberseguridad, y el grado de avance hacia la adecuación al ENS.
- Adaptación al ENS mediante autoevaluaciones, revisión de evidencias, simulacros, asesoramiento técnico sobre medidas de adecuación, y acompañamiento al proceso completo de auditoría externa hasta la obtención del certificado (siempre dentro de la duración del contrato) en cinco (5) ayuntamientos.
- Apoyo al modelo de gobernanza regional en ciberseguridad, con el diseño de mecanismos de coordinación, supervisión y mejora continua aplicables de forma transversal en el sector local, y su integración en el Comité de Seguridad de la Información de la Comunidad de Madrid a través de grupos sectoriales específicos.

Resultados esperados e impacto previsto

El presente contrato tiene como finalidad lograr una transformación estructural, homogénea y sostenible en la gestión de la seguridad de la información en el entorno de los ayuntamientos de menos de 20.000 habitantes de la Comunidad de Madrid, en cumplimiento de los requisitos del Esquema Nacional de Seguridad y orientada a la creación de una capacidad organizativa sólida y coordinada frente a riesgos cibernéticos. Los resultados esperados se agrupan en los siguientes ejes:

- Un mapa del riesgo actual de los ayuntamientos. Y un marco de gestión de este mapa, para ver los avances en la materia a futuro. Con una propuesta de aquellos ayuntamientos que pueden beneficiarse de este refuerzo de la ciberseguridad.



- Consolidación de un modelo común de Sistema de Gestión de Seguridad de la Información en el ámbito local, formalizado, documentado y verificable, compatible con auditorías de certificación ENS.
- Definición de un conjunto completo de modelos de políticas, procedimientos y estructuras de control homogéneas, específicamente adaptadas al sector local para su despliegue en 35 ayuntamientos.
- Trabajos orientados a la adaptación al ENS en al menos 5 ayuntamientos, mediante un servicio integral que incluya:
 - Autoevaluaciones iniciales y finales.
 - Revisión documental y análisis de evidencias.
 - Asesoramiento técnico y apoyo a la implantación de medidas correctoras.
 - Acompañamiento en la ejecución de auditorías externas por parte de auditores independientes conforme a lo previsto en el ENS.
- Implantación de un modelo de gobernanza y supervisión sectorial, con:
 - Constitución y dinamización de los Comités de Seguridad en los ayuntamientos y refuerzo del comité regional.
 - Formalización de las tres líneas de defensa, con trazabilidad estructurada de decisiones.
 - Propuesta de modelo operativo sostenible tras la finalización del proyecto.

II.1. REQUISITOS FUNCIONALES

A lo largo de esta cláusula se describen, estructuradas en tres grandes bloques funcionales, las actividades a ejecutar por la empresa adjudicataria, incluyendo para cada una de ellas su finalidad, el contenido mínimo exigido, los entregables esperados y, cuando aplique, los criterios de calidad o resultado que permitirán verificar su correcta ejecución. Las actividades no se asocian a personas concretas, sino que deberán prestarse en régimen de servicio profesional, con plena capacidad técnica, autonomía operativa y vocación de sostenibilidad del modelo construido.

Bloque 1. Planificación y despliegue del sistema de gestión regional de seguridad de información

Este bloque comprende las actividades orientadas a diseñar, estructurar e implantar el SGSI a nivel regional, bajo responsabilidad de la Agencia de Ciberseguridad. Incluye el desarrollo del marco documental, metodológico y organizativo, asegurando una base común y escalable para su posterior despliegue en las entidades locales.

El adjudicatario deberá diseñar e implantar el Sistema de Gestión de la Seguridad de la Información de la Agencia de Ciberseguridad, que actuará como unidad de referencia y supervisión del modelo regional.

El SGSI deberá basarse en la norma ISO/IEC 27001:2022 como marco de gestión, asegurando de forma expresa el cumplimiento íntegro de los requisitos y medidas establecidos en el Esquema Nacional de Seguridad, de conformidad con lo dispuesto en el Real Decreto 311/2022. La implantación deberá garantizar que todos los elementos exigidos por el ENS se encuentran implementados, documentados y operativos dentro de la estructura del SGSI.

Las actividades a realizar incluyen, como mínimo:



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

- **Definición de la estructura documental del SGSI**, incluyendo políticas, procedimientos, normas, instrucciones, modelos de registro, inventarios y controles, organizados en torno a las fases del ciclo de vida de la seguridad de la información.
- **Identificación y categorización de los activos esenciales y servicios soportados**, tanto los internos de la Agencia como aquellos vinculados a sus funciones de supervisión, coordinación y apoyo al sistema regional.
- **Establecimiento del marco de gobernanza**, con definición del Comité de Seguridad de la Información, responsables de seguridad, responsables del SGSI, canales de coordinación y responsabilidades internas.

Los resultados esperados son los siguientes:

- a. Un modelo de SGSI completo, documentado y operativo, aprobado formalmente por el órgano de gobierno de la Agencia que corresponda.
- b. Evidencias verificables del cumplimiento pleno de los controles y requisitos del ENS, con una estructura y operativa alineadas con la ISO/IEC 27001:2022.

Bloque 2. Soporte a la certificación ENS en entidades seleccionadas

Este bloque comprende las actividades específicas de auditoría que permitirán a **cinco entidades locales avanzar hacia la certificación del Esquema Nacional de Seguridad**, en los términos establecidos por la normativa aplicable y las guías técnicas del CCN. Las actividades previstas se ajustan a un ciclo completo de auditoría, incluyendo la evaluación inicial de preparación, la ejecución de auditorías internas, la validación de acciones correctoras, y el acompañamiento a aquellas entidades que opten por una auditoría externa con un tercero acreditado. Todas las fases se realizarán conforme a criterios de independencia, trazabilidad y uniformidad metodológica, asegurando la validez técnica de los resultados y su integración en la supervisión regional del cumplimiento del ENS. La selección de las entidades será realizada por la Agencia en función de criterios estratégicos y del grado de madurez alcanzado por cada una durante la primera fase del contrato.

2.1 Evaluación de preparación para auditoría (pre-auditoría técnica)

El adjudicatario deberá realizar una evaluación técnica inicial en cada una de las entidades seleccionadas para la certificación ENS, con el objetivo de verificar su grado real de preparación para afrontar una auditoría formal conforme a los requisitos del Esquema Nacional de Seguridad. Esta pre-auditoría no tendrá carácter certificador ni implicará el inicio de la auditoría interna o de tercera parte, sino que constituirá una revisión técnica detallada y objetiva del estado de cumplimiento alcanzado.

Las actuaciones mínimas a desarrollar en esta fase incluyen:

- **Revisión exhaustiva del marco documental del SGSI**, prestando especial atención a la coherencia, completitud y actualización de políticas, procedimientos, registros y evidencias vinculadas a los controles exigidos por el ENS.
- **Verificación técnica y organizativa del cumplimiento de medidas**, mediante entrevistas, revisión de configuraciones, trazabilidad de procesos, y contraste de evidencias que sustenten la efectividad de las salvaguardas implantadas.
- **Identificación de deficiencias o desviaciones** respecto a los requisitos del ENS (según su categoría aplicable), clasificando las observaciones por gravedad y urgencia.



- **Propuesta estructurada de acciones correctoras**, incluyendo medidas prioritarias para alcanzar un nivel aceptable de preparación antes de iniciar la auditoría formal.
- **Informe de evaluación de preparación**, emitido por el equipo auditor del adjudicatario, con una visión clara y trazable del grado de cumplimiento actual y los pasos recomendados para avanzar con garantías hacia la certificación.

Este informe será presentado a los responsables de la entidad y a la Agencia de Ciberseguridad, y servirá de base para la decisión conjunta sobre la viabilidad de continuar con el proceso de auditoría interna o de certificación en esa entidad.

Los resultados esperados de esta actividad son:

- a. Informe técnico detallado del estado de preparación de cada entidad para la auditoría ENS.
- b. Relación de no conformidades y desviaciones detectadas, con propuestas de subsanación.
- c. Recomendación formal sobre la viabilidad de iniciar el proceso de auditoría, con trazabilidad respecto a los requisitos del ENS.

2.2 Auditoría interna completa

El adjudicatario deberá llevar a cabo la auditoría interna completa del sistema de gestión de seguridad de la información de cada una de las entidades seleccionadas para la certificación, conforme a los principios de independencia, objetividad y rigor técnico establecidos en el Esquema Nacional de Seguridad y en las normas ISO/IEC 27001 e ISO/IEC 19011.

Esta auditoría interna deberá reproducir fielmente el esquema metodológico, estructural y documental empleado en las auditorías de certificación, en atención a las directrices del Centro Criptológico Nacional (CCN), garantizando así su utilidad como ensayo previo y realista del proceso de certificación formal. La estructura, los procedimientos y los criterios utilizados deberán ser equivalentes a los exigidos a una auditoría de tercera parte.

Las actividades mínimas a desarrollar incluyen:

- Planificación formal de la auditoría, con definición de alcance, objetivos, criterios, cronograma y recursos, siguiendo el formato previsto para auditorías de certificación, y su validación por parte de la Agencia y de la entidad auditada.
- Revisión documental completa, incluyendo el marco normativo interno, evidencias del SGSI, resultados de análisis de riesgos, planes de tratamiento, medidas implantadas, acciones de seguimiento y cumplimiento de los controles del ENS.
- Entrevistas estructuradas con los responsables de seguridad, tecnología, protección de datos y usuarios clave, orientadas a verificar tanto la implantación como la eficacia de las medidas de seguridad.
- Verificación técnica y organizativa in situ, mediante observación directa, revisión de configuraciones, análisis de evidencias, trazabilidad documental y comprobación del funcionamiento operativo de controles relevantes.
- Registro y clasificación de hallazgos, identificando no conformidades, observaciones y oportunidades de mejora, conforme a la tipología y severidad establecidas por el CCN para las auditorías ENS.



- Elaboración del informe de auditoría interna, con una estructura equivalente al informe requerido para la certificación, incluyendo grado de cumplimiento, resumen ejecutivo, detalle de hallazgos, evidencias asociadas y recomendaciones.

Los resultados esperados de esta actividad son:

- a. Informe de auditoría interna estructurado según el modelo de certificación, incluyendo hallazgos clasificados y recomendaciones.
- b. Determinación precisa del grado de conformidad de la entidad con el ENS, como referencia directa para afrontar la auditoría de certificación con garantías.

2.3 Apoyo a auditoría de certificación externa por terceros

En los casos en que, de forma conjunta entre la Agencia de Ciberseguridad y la entidad correspondiente, se determine que la auditoría de certificación del Esquema Nacional de Seguridad será llevada a cabo por una entidad certificadora externa, el adjudicatario deberá proporcionar todo el acompañamiento técnico, documental y organizativo necesario hasta la obtención de la certificación (siempre dentro de la duración del contrato).

Las actividades mínimas a desarrollar por el adjudicatario incluyen:

- Coordinación y planificación conjunta con la entidad certificadora resultante del proceso de contratación, definiendo alcance, criterios de auditoría, agenda de trabajo y logística necesaria.
- Preparación técnica y documental de la entidad auditada, asegurando que toda la evidencia requerida por la entidad certificadora esté completa, actualizada, accesible y trazable.
- Organización de la auditoría, incluyendo gestión de agendas, convocatorias de entrevistas y disposición de entornos para demostraciones técnicas.
- Acompañamiento durante el desarrollo de la auditoría, dando soporte en tiempo real para la localización de evidencias, resolución de dudas del auditor externo y correcta articulación de respuestas por parte de la entidad auditada.
- Seguimiento de hallazgos preliminares, apoyando en la interpretación técnica de no conformidades y en la elaboración de planes de acción correctiva.
- Revisión técnica del informe preliminar emitido por la entidad certificadora, en coordinación con la entidad auditada, antes de su cierre definitivo.

Los resultados esperados de esta actividad son:

- a. Entidad auditada completamente preparada y acompañada durante todo el proceso de certificación externa.
- b. Coordinación eficaz con la organización certificadora, con planificación y logística alineadas a sus requisitos.
- c. Evidencia documental y técnica estructurada y presentada conforme a los criterios del auditor externo.
- d. Apoyo en la resolución de hallazgos y preparación de acciones correctoras cuando proceda, hasta la obtención de la conformidad.

2.4 Validación de acciones correctoras y cierres de hallazgos

Tras la realización de auditorías internas o externas de certificación del Esquema Nacional de Seguridad, el adjudicatario deberá prestar apoyo técnico especializado para la validación y cierre



de las acciones correctoras definidas con el fin de resolver los hallazgos identificados. Este proceso deberá asegurar que las acciones se implementan de forma eficaz, que su ejecución queda debidamente documentada y que cumplen con los requisitos de cierre establecidos por el ENS y por el organismo auditor correspondiente, siempre dentro de la duración del Contrato. En caso de que ciertas medidas correctoras requieran de la aplicación directa de acciones técnicas por parte directa de las entidades, serán estas entidades las responsables de su ejecución, para lo que deberán dedicar recursos y medios. No obstante, el adjudicatario deberá prestarle el máximo apoyo y asesoramiento para que la ejecución de dichas medidas sea lo más sencilla y efectiva posible.

Este alcance comprende tanto los hallazgos detectados en auditorías internas realizadas por el propio adjudicatario, como aquellos generados en auditorías externas desarrolladas por entidades certificadoras.

Las funciones mínimas a desarrollar incluyen:

- Análisis y clasificación de hallazgos (no conformidades, observaciones u oportunidades de mejora), determinando conjuntamente con la entidad auditada su naturaleza, criticidad y plazos de resolución.
- Revisión técnica y documental de las acciones correctoras propuestas, verificando su adecuación, eficacia y coherencia con los requisitos del ENS y con las buenas prácticas de ciberseguridad.
- Supervisión de la ejecución de las acciones correctoras, acompañando su implantación, resolviendo dudas técnicas y validando los resultados obtenidos.
- Consolidación de evidencias de cierre, garantizando su organización, trazabilidad y suficiencia para su presentación formal ante el equipo auditor.
- Apoyo en la elaboración de la documentación de cierre, incluyendo informes de cierre, actualizaciones del plan de acción y, cuando proceda, declaraciones de conformidad.
- Coordinación con el organismo auditor para la revisión final y aceptación del cierre de hallazgos.

Los resultados esperados de esta actividad son:

- a. Validación técnica y formal del cierre de los hallazgos identificados en auditorías ENS.
- b. Registro completo y verificable de las acciones correctoras adoptadas.

Bloque 3. Gobierno de la seguridad, comités y visibilidad del riesgo

Este bloque comprende las actividades orientadas a reforzar y articular la gobernanza de la seguridad de la información en el conjunto del sistema regional, impulsando la coordinación entre entidades, la eficacia de los comités de seguridad y la adecuada visibilidad del riesgo a todos los niveles.

Incluye la dinamización y apoyo a los Comités de Seguridad de la Información (CSI) de las entidades, el fortalecimiento del Comité de Seguridad de la Información de la Comunidad de Madrid como órgano de referencia regional, la correcta organización de las funciones y responsabilidades bajo el modelo de las tres líneas de defensa, la consolidación de información de supervisión mediante cuadros de mando, y las acciones de comunicación y visibilidad necesarias para asegurar la sostenibilidad del modelo.



3.1 Dinamización de Comités de Seguridad locales

El adjudicatario deberá impulsar, coordinar y dar soporte a los Comités de Seguridad de la Información de las entidades locales participantes, asegurando que funcionen como órganos activos de coordinación, seguimiento y toma de decisiones en materia de seguridad de la información y ciberseguridad.

Estas actividades estarán orientadas a reforzar la participación de los responsables y equipos designados, mejorar la eficacia de las reuniones, y garantizar la alineación de los trabajos con las directrices regionales emitidas por la Agencia de Ciberseguridad.

Las funciones mínimas a desarrollar incluyen:

- Asistencia técnica en la constitución o reactivación de los CSI, asegurando la designación de sus miembros y la definición clara de roles y responsabilidades.
- Preparación y distribución de agendas normalizadas, documentación de trabajo y material de apoyo para cada reunión, de acuerdo con el calendario establecido con la entidad.
- Apoyo en la dirección o moderación de las reuniones cuando así lo solicite la entidad, velando por la consecución de los objetivos y el cumplimiento de los tiempos previstos.
- Seguimiento y verificación del cumplimiento de acuerdos y acciones derivadas de cada CSI, registrando su estado de avance y manteniendo la trazabilidad de las decisiones adoptadas.
- Integración de los temas y acuerdos relevantes en los canales de coordinación con el Comité de Seguridad de la Información de la Comunidad de Madrid, facilitando el flujo de información entre niveles local y regional.

Los resultados esperados de esta actividad son:

- a. Comités de Seguridad de la Información constituidos y activos en todas las entidades locales incluidas en el proyecto.
- b. Reuniones periódicas documentadas, con acuerdos y acciones registradas y trazables.
- c. Participación efectiva de los CSI locales en la coordinación regional, contribuyendo a la coherencia y sostenibilidad del modelo de gobernanza de la seguridad.

3.2 Reforzamiento del Comité de Seguridad de la Información de la Comunidad

El adjudicatario deberá prestar apoyo a la Agencia de Ciberseguridad en la ampliación y fortalecimiento del Comité de Seguridad de la Información de la Comunidad de Madrid, de acuerdo con su orden de creación y normativa reguladora, con el fin de integrar de manera efectiva a las entidades municipales y garantizar su funcionamiento bajo un marco de gobernanza común.

Esta ampliación comprenderá la creación de uno o varios grupos específicos que aglutinen a las entidades participantes, asegurando la coordinación interna del sector y su integración progresiva en la estructura general del Comité. El modelo de funcionamiento deberá contemplar particularidades normativas, operativas y tecnológicas del ámbito local.

Las funciones mínimas a desarrollar incluyen:

- Asistencia técnica en la definición y constitución de los grupos sectoriales dentro del Comité, incluyendo criterios de composición, funciones, canales de comunicación y frecuencia de reuniones.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

- Adaptación de la metodología de trabajo del Comité para incorporar un modo de funcionamiento específico para el sector local, asegurando que sus particularidades se reflejen en las agendas, en el seguimiento de acuerdos y en la priorización de acciones.
- Coordinación con los Comités de Seguridad de la Información locales de los municipios para consolidar su participación y representar de forma unificada las necesidades del sector en el Comité regional.

Los resultados esperados de esta actividad son:

- a. Comité de Seguridad de la Información de la Comunidad de Madrid ampliado, con grupos sectoriales formalmente constituidos y operativos.
- b. Participación efectiva de las entidades municipales en la gobernanza regional de la seguridad de la información, con coordinación fluida entre niveles local, sectorial y regional.

II.2. REQUISITOS NO FUNCIONALES

En este apartado se definen los requisitos no funcionales que deben cumplir las actividades desarrolladas en el marco del contrato específico. Se refieren tanto a las condiciones técnicas de los trabajos como a la metodología de ejecución, el control de calidad y la gestión del proyecto.

II.2.1. REQUISITOS TÉCNICOS

- Las actividades desarrolladas deberán respetar los principios de interoperabilidad, seguridad y trazabilidad propios de la administración electrónica, y ser compatibles con los sistemas y herramientas utilizados por la Agencia de Ciberseguridad de la Comunidad de Madrid y las entidades objeto del alcance.
- Toda la documentación generada deberá elaborarse en formatos abiertos, reutilizables y editables, preferentemente en versiones compatibles con LibreOffice o Microsoft Office.
- Se deberán garantizar la confidencialidad, integridad y disponibilidad de la información tratada, de acuerdo con el marco del Esquema Nacional de Seguridad (ENS).
- El contratista deberá aplicar buenas prácticas de gestión documental, garantizando la organización lógica de los contenidos, el versionado adecuado y la identificación clara de autores, fechas y niveles de revisión.
- Las herramientas o entornos que se propongan para el desarrollo de modelos, plantillas, informes u otros productos deberán ser tecnológicamente compatibles con el entorno TIC de la Agencia, y no requerirán licencias adicionales por parte de la Administración, salvo autorización expresa.

II.2.2. METODOLOGÍA

- El enfoque metodológico deberá ser flexible, incremental y basado en la mejora continua, tomando como referencia el ciclo PDCA (Plan-Do-Check-Act).
- Se priorizará el uso de buenas prácticas internacionales en auditoría, gobernanza y gestión de la seguridad de la información, tales como:



- ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005
- ISO 19011 (Directrices para la auditoría de sistemas de gestión)
- COBIT, ITIL, MAGERIT o marcos de control similares.
- El contratista deberá adaptar la metodología a las directrices y decisiones técnicas de la Agencia, que mantiene la responsabilidad sobre el enfoque global del programa de trabajo.
- La metodología propuesta deberá estar orientada a resultados y a la generación de productos reutilizables, que aporten valor a la evolución del sistema de gestión de seguridad de la información.

II.2.3. CALIDAD DE LOS DESARROLLOS

- El servicio deberá incorporar mecanismos de revisión técnica y validación documental de los entregables, que garanticen la calidad, consistencia y utilidad operativa de los productos generados.
- Se establecerán criterios de calidad en relación con:
 - Exhaustividad y corrección técnica.
 - Claridad y estructura documental.
 - Trazabilidad y justificación de los contenidos.
- La Agencia podrá solicitar al contratista la aplicación de planes de mejora, revisión o reformulación de entregables que no cumplan los niveles de calidad esperados.
- El contratista deberá mantener una actitud proactiva en la detección de errores, incoherencias o desviaciones, proponiendo acciones correctoras cuando proceda.

II.2.4. GESTIÓN DEL PROYECTO

- La ejecución del contrato deberá desarrollarse conforme a principios profesionales de gestión de proyectos, aplicando prácticas derivadas de marcos como PMBOK o PRINCE2.
- Se designará un responsable de proyecto por parte del contratista, que actuará como interlocutor técnico único ante la Agencia, gestionará el equipo de trabajo y asegurará el cumplimiento de los plazos y entregables.
- Se establecerán reuniones periódicas de seguimiento con la Agencia, con periodicidad mensual o según se acuerde, en las que se revisará el estado de avance, se identificarán desviaciones y se acordarán las prioridades para el periodo siguiente.
- El contratista deberá mantener actualizado un registro interno de actividades, accesible para la Agencia a efectos de control, y documentar adecuadamente cada entregable y cada hito del servicio.

II.3. HITOS Y ENTREGABLES

Dado el carácter técnico y de apoyo transversal del servicio, los **hitos y entregables** se estructuran en bloques de trabajo coherentes con la planificación prevista para la duración del contrato (4 meses), permitiendo el seguimiento del grado de avance, la validación de resultados intermedios y la trazabilidad de las actividades realizadas.



La autenticidad de este documento se puede comprobar en
<https://gestion.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

La siguiente planificación podrá ser ajustada en función de la evolución del programa de trabajo y las necesidades de la Agencia, siempre bajo supervisión de la Agencia. Y teniendo en cuenta que al ser fondos RETECH el pago se tiene que realizar antes del 31 de Junio del 2026.

Hito	Descripción del hito	Fecha aprox.	Porcentaje de ejecución	Importe facturable
HITO_01	Definición del SGSI de la Agencia y planificación del soporte	T0 + 1 meses	21,67%	El 21,67% de la Oferta Económica
HITO_02	Pre-auditorías técnicas	T0 + 2 mes	33,33%	El 33,33% de la Oferta Económica
HITO_03	Auditorías internas completas	T0 + 3 mes	33,33%	El 33,33% de la Oferta Económica
HITO_04	Apoyo a auditorías de certificación e Informes de supervisión y gobernanza regional	T0 + 4 mes	11,67%	El 11,67% de la Oferta Económica

El porcentaje de ejecución indicado representa tanto el porcentaje alcanzado en el hito sobre el plazo total del contrato como el porcentaje estimado del esfuerzo total, dado que se considera una distribución uniforme del esfuerzo a lo largo de la duración del contrato.

Entregables por Hito:

Hito	Entregable	Observaciones
HITO_1	E1 Bloque 1. Modelo funcional y organizativo del SGSI	Deberá contener el diseño del modelo de referencia del Sistema de Gestión de la Seguridad de la Información para la Agencia, que incluya el SGSI del resto de entidades. Incluye estructura organizativa, roles y responsabilidades, políticas, procesos, procedimientos, métricas y mecanismos de supervisión. Integra el marco ENS, NIS2 y RGPD. Los criterios de aceptación son: 1. Inclusión de todos los procesos y roles clave definidos. 2. Trazabilidad con requisitos normativos (ENS, NIS2, RGPD). 3. Validación por la Agencia sin observaciones críticas.
HITO_1	E2 Bloque 2. Metodología y planificación de auditorías	Documento que defina el procedimiento común para realizar auditorías internas y de certificación ENS en las entidades del alcance (5), alineado con el ENS, normas ISO/IEC aplicables y guías CCN-STIC. Debe incluir la descripción detallada de las fases, criterios de evaluación, roles y responsabilidades, formatos de recogida de evidencias y un plan anual con el calendario de auditorías para todas las entidades. Los criterios de aceptación son: 1. Inclusión de fases completas: planificación, ejecución, informe y seguimiento. 2. Criterios y referencias normativas claramente identificados. 3. Roles y responsabilidades definidos para cada fase. 4. Formatos y plantillas normalizados y validados por la Agencia. 5. Plan de auditorías aprobado por la Agencia.
HITO_2	E3 Bloque 2. Pre-auditorías técnicas para las 5 entidades seleccionadas para	Informe que recoja el resultado de la evaluación inicial del estado de preparación de cada entidad para el proceso de certificación ENS. El informe deberá identificar brechas, debilidades y áreas de mejora, y determinar si la entidad se encuentra en condiciones



Hito	Entregable	Observaciones
	certificación ENS	de avanzar hacia dicho proceso. Los criterios de aceptación son: 1. Cobertura de todas las entidades determinadas para avanzar en el proceso de certificación. 2. Diagnóstico individual con recomendaciones específicas y una conclusión clara sobre la preparación para avanzar en el proceso. 3. Formato y contenido validados por la Agencia
HITO_3	E4 Bloque 2. Auditorías internas completas para las 5 entidades seleccionadas para certificación ENS	Informe completo de estado de adaptación previo a la auditoría externa de certificación: 1. Informe de auditoría interna estructurado según el modelo de certificación, incluyendo hallazgos clasificados y recomendaciones. 2. Determinación precisa del grado de conformidad de la entidad con el ENS, como referencia directa para afrontar la auditoría de certificación con garantías
HITO_4	E5 Bloque 2. Apoyo a auditoría de certificación externa para las 5 entidades seleccionadas para certificación ENS	Informe completo donde se evidencie: 1. Entidad auditada completamente preparada y acompañada durante todo el proceso de certificación externa. 2. Coordinación eficaz con la organización certificadora, con planificación y logística alineadas a sus requisitos. 3. Evidencia documental y técnica estructurada y presentada conforme a los criterios del auditor externo. Apoyo en la resolución de hallazgos y preparación de acciones correctoras cuando proceda, hasta la obtención de la conformidad
HITO_4	E6 Bloque 3. Informes de supervisión y gobernanza regional	Conjunto de informes que documenten el estado, evolución y efectividad de la gobernanza de la seguridad de la información en el marco del ámbito local. Estos informes deberán evidenciar la constitución y actividad de los Comités de Seguridad de la Información (locales y regional), la aplicación del modelo de tres líneas de defensa, la coordinación sectorial y regional, así como la visibilidad del riesgo mediante el Índice de Riesgo Regional (IRR) y sus subindicadores. Los criterios de aceptación son: 1. Comités de Seguridad de la Información constituidos y activos en todas las entidades locales incluidas en el proyecto. 2. Reuniones periódicas documentadas, con acuerdos y acciones registradas y trazables. 3. Comité de Seguridad de la Información de la Comunidad de Madrid ampliado. 4. Participación efectiva de las entidades del sector local en la gobernanza regional de la seguridad de la información, con coordinación fluida entre niveles local, sectorial y regional

ANEXO III SERVICIOS DE MANTENIMIENTO PARA ASEGURAR LA CONTINUIDAD DE SISTEMAS EN ENTORNOS PRODUCTIVOS

No aplica. El objeto del presente contrato no contempla el desarrollo ni el mantenimiento de sistemas en entornos productivos, por lo que no son de aplicación las cláusulas contenidas en este anexo.



III.1. DESCRIPCIÓN DEL SERVICIO DE MANTENIMIENTO PARA ASEGURAMIENTO DE LA CONTINUIDAD DEL SERVICIO DE LOS SISTEMAS EN ENTORNOS PRODUCTIVOS

No aplica.

III.2. DIMENSIONAMIENTO DEL SERVICIO

No aplica.

III.3. ACUERDOS DE NIVEL DE SERVICIO

No aplica.

ANEXO IV MODELO DE GESTIÓN Y DEFINICIÓN DE UNIDADES DE TRABAJO

No aplica.

El objeto del presente contrato no contempla el desarrollo, mantenimiento ni evolución de sistemas de información que requiera la aplicación de Unidades de Trabajo (UTs) como método de medición de esfuerzo.

El servicio se estructura en torno a tareas de análisis, consultoría técnica y soporte metodológico en materia de auditoría, cuyas prestaciones se organizan por hitos y entregables definidos, conforme a la programación y al alcance establecido en el Anexo II del presente documento.

ANEXO V REQUISITOS DE LOS PERFILES PROFESIONALES

El propuesto a 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.

Jefe de Proyecto (Especialidad Seguridad)

- **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 (Projects 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, auditoría 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.

Consultor (Especialidad 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 una (1) certificación 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 modelos de SGSI.
 - 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.

Consultor (Cumplimiento Legal)

- **Formación:** Título universitario MECES 2 o superior en áreas técnicas relacionadas con ciberseguridad, tecnologías de la información o auditoría.
- **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, normas y procedimientos internos y normativas relacionadas con la ciberseguridad y la protección de datos.

Analista (Especialidad 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.

ANEXO VI CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

El presente contrato específico tiene por objeto la prestación de un servicio, cuyo objetivo es el desarrollo y/o mantenimiento de uno o varios sistemas de información. No tiene por objeto la explotación ni la operación en producción de dicho sistema de información.

A efectos del artículo 11 del RD 311/2022, en adelante ENS, el responsable del sistema es el Responsable del Contrato Específico indicado en el apartado 1 del presente documento de invitación.

En cumplimiento del artículo 13.5 del ENS, es obligación del adjudicatario designar una Persona de Contacto (POC) que canalice y supervise el cumplimiento de los anteriores requisitos y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes de seguridad en el ámbito de dicho servicio de desarrollo. Dicha Persona de Contacto será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en el organismo destinatario de la prestación.

El organismo destinatario informará de sus deberes, obligaciones y responsabilidades en materia de seguridad en lo relativo al sistema de información al personal puesto a disposición del servicio por el adjudicatario, en cumplimiento del artículo 15 del ENS. Esta información se realizará una vez iniciada la ejecución del contrato. Es obligación del adjudicatario supervisar la



actuación de dicho personal, para verificar que se siguen los procedimientos establecidos por el organismo, se aplican las normas indicadas y los procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

En aplicación del artículo 16 del ENS, se han determinado los requisitos de formación y experiencia del personal implicado en la ejecución del contrato que se han indicado en el Anexo V.

Medidas del Anexo II del RD 311/2022 que son de aplicación al presente contrato específico:

1) Sistemas de categoría BÁSICA:

- a. El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo. El organismo destinatario dispone de estos entornos y proporcionará las normas de uso, junto con el resto de información que proporcionará al inicio de la ejecución del contrato específico.

2) Sistemas de categoría MEDIA:

- a. Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.
- b. Se aplicará una metodología de desarrollo seguro reconocida que:
 - i. Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
 - ii. Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (overflow).
 - iii. Tratará específicamente los datos usados en pruebas.
 - iv. Permitirá la inspección del código fuente.
- c. Se aplicará el principio de seguridad integral desde el diseño del sistema, especialmente:
 - i. Los mecanismos de identificación y autenticación.
 - ii. Los mecanismos de protección de la información tratada.
 - iii. La generación y tratamiento de pistas de auditoría.
- d. Las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales, el organismo destinatario impartirá las oportunas instrucciones para garantizar el nivel de seguridad correspondiente. Es obligación del adjudicatario asegurarse de que el personal asignado al servicio cumple dichas instrucciones.
- e. Es obligación del adjudicatario elaborar y mantener actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. El adjudicatario mantendrá un histórico de los componentes utilizados en las diferentes versiones del software durante todo el periodo de ejecución del contrato específico. El contenido mínimo de la lista de componentes contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, y en su caso, se adecuará a lo descrito en la correspondiente Guía CCN-STIC en su versión más actualizada.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1000827126708388116787**

ANEXO VII MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN

D., con DNI o documento equivalente en caso de extranjeros o. pasaporte nº....., en su propio nombre, o como representante legal de la empresa adjudicataria del CONTRATO ESPECÍFICO Nº del SISTEMA DINÁMICO PARA LOS SERVICIOS DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN A MEDIDA O DE APLICACIONES DE GESTIÓN (SDA 26/2021; Expediente 2021/16), pongo en conocimiento del órgano de contratación, a los efectos del artículo 215.2.b) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), que, para la prestación indicada, se subcontrata con la/s siguiente/s entidad/es:

(Indicar:

- *Los sujetos intervinientes (identidad, datos de contacto y representantes legales) en el subcontrato, con indicación de la capacidad técnica y profesional del subcontratista o en su caso, clasificación, justificativa de la aptitud para prestar parte del servicio.*
- *Indicación del objeto o partes del contrato a realizar por cada uno de los subcontratistas.*
- *Importe del subcontrato y porcentaje que representa la prestación parcial sobre el precio del contrato principal.*
- *Importe acumulado de subcontratación, en porcentaje, que se alcanzará con el presente subcontrato sobre el precio del contrato principal.*
- *Plazos en los que el subcontratista se obliga a pagar a los subcontratistas el precio pactado.)*

Asimismo, hago constar que en la celebración del/los subcontrato/s se cumplirán los requisitos establecidos en el artículo 216 de la LCSP.

A la presente comunicación se acompaña la siguiente documentación relativa a los subcontratistas:

- **Declaración responsable** de los subcontratistas de no hallarse incurso en prohibición de contratar, conforme el art. 71 de la LCSP.⁶
- **Certificación positiva** de la Agencia Estatal de Administración Tributaria de hallarse los subcontratistas al corriente en el cumplimiento de las obligaciones tributarias o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.
- **Certificación positiva** de la Tesorería General de la Seguridad Social de hallarse los subcontratistas al corriente de sus obligaciones con la Seguridad Social o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a de de

Firmado electrónicamente

⁶ La declaración responsable deberá formularse en los siguientes términos “**Que ni el firmante de la declaración, ni la persona física/jurídica a la que representa, ni ninguno de sus administradores o representantes se hallan incursos en supuesto alguno a los que se refiere el artículo 71 de la LCSP.**”

