

**SISTEMA DINÁMICO DE ADQUISICIÓN DE SUMINISTROS DE SOFTWARE
DE SISTEMA, DE DESARROLLO Y DE APLICACIÓN, DEL SISTEMA ESTATAL
DE CONTRATACIÓN CENTRALIZADA - SDA 25/2022**

(Expediente nº 2022/48)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

Suministro de Licenciamiento de software para una
solución SIEM SOAR-SOC de SOCs para las entidades de la
región, en el marco del PRTR, co-financiado por la unión
europea – NextGenerationEU

Lote 4 - Software de ciberseguridad

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 naturales contados a partir del día siguiente a la fecha de 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://gestion.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

TÉRMINOS Y CONDICIONES

1.	ORGANISMO DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO	4
2.	LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO	4
2.1.	Lote, título y objeto	4
2.2.	Características principales de las prestaciones	4
2.3.	Tratamiento de datos de carácter personal por parte del adjudicatario	5
2.4.	Categorización conforme al Esquema Nacional de Seguridad (ENS)	5
2.5.	Tratamientos de datos personales para los programas en modalidad de nube	6
3.	DURACIÓN DEL CONTRATO	7
3.1.	Fecha de inicio de la ejecución	7
3.2.	Plazo de entrega de las licencias	7
3.3.	Plazo de ejecución del contrato	7
3.4.	Prórroga del contrato específico	8
4.	VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN	8
4.1.	Presupuesto de licitación y aplicaciones presupuestarias	8
4.2.	Determinación del precio del contrato	9
4.3.	Tramitación del expediente (a efectos presupuestarios)	10
4.4.	Modificación del contrato específico	11
4.5.	Valor estimado	11
4.6.	Contrato financiado con cargo al presupuesto de la Unión Europea	11
5.	LUGAR Y CONDICIONES DE LA ENTREGA	12
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN	12
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	13
7.1.	Ponderación de los criterios de adjudicación	13
7.2.	Fórmula aplicable al criterio precio	13
7.3.	Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio	14
7.3.1.	Criterios evaluables automáticamente mediante fórmulas	14
7.3.2.	Fórmulas para la evaluación automática de los criterios	14
7.4.	Criterios cuya cuantificación depende de un juicio de valor	16
7.4.1.	Criterios y ponderación	17
7.4.2.	Método de valoración y documentación	17
8.	OFERTAS ANORMALMENTE BAJAS	18
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA	19
9.1.	Obligaciones generales	19
9.2.	Otras condiciones de ejecución del contrato	19
9.3.	Obligaciones de seguridad en cumplimiento del ens	20
9.4.	Obligaciones relativas al cumplimiento de las condiciones de los programas ofertados en modalidad de nube cuando exista tratamiento de datos personales	20
10.	PAGO Y FACTURACIÓN	21
10.1.	Pago del precio	21



10.2.	Condiciones de presentación de las facturas	22
11.	GARANTÍA DE LOS BIENES	23
12.	PENALIDADES	23
12.1.	Penalidades fijadas en el sistema dinámico de adquisición	23
12.2.	Fórmula para la aplicación de penalidades	24
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	24
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS	24
ANEXO I PRESCRIPCIONES TÉCNICAS		28
I.1.	Requisitos funcionales de los programas a suministrar	28
I.2.	Requisitos no funcionales de los programas a suministrar	34
I.3.	Periodo de vigencia y modalidad de licenciamiento	34
I.4.	Requisitos de seguridad de los programas en la nube	35
ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO		36
II.1.	Servicios de instalación avanzada de los programas a suministrar	36
II.2.	Servicios de soporte de los programas a suministrar	38
II.2.1.	Dimensionamiento del servicio.....	39
II.2.2.	Acuerdos de nivel de servicio.....	39
II.3.	Requisitos de los perfiles profesionales	41
ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS		41
III.1.	Tratamientos de datos y finalidad de los tratamientos	41
III.2.	Medidas técnicas y organizativas.....	41
ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE		42
ANEXO V MODELO DE DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos		44
ANEXO VI Manifestación de conformidad del responsable del tratamiento DE LOS DATOS DEL ORGANISMO DESTINATARIO		46
ANEXO VII ENTREGAS PARCIALES.....		47
ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO		47
ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN		48
ANEXO X DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA		49
ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA		52
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea	52
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR.....	54



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

Organismo destinatario

Unidad proponente: **Agencia de Ciberseguridad de la Comunidad de Madrid**
Centro directivo: **Agencia de Ciberseguridad de la Comunidad de Madrid**
Departamento/organismo: **Agencia de Ciberseguridad de la Comunidad de Madrid**

Responsable del contrato (nombre, apellidos, cargo y dependencia orgánica):

D. 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: **915 80 50 01**

Órgano de Contratación:

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

2. LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO

2.1. LOTE, TÍTULO Y OBJETO

Lote objeto de licitación: **Lote 4 - Software de ciberseguridad**

Título del contrato: “Suministro de Licenciamiento de software para una solución SIEM SOAR-SOC de SOC para las entidades de la región, en el marco del PRTR, co-financiado por la unión europea – NextGenerationEU ”

Objeto del contrato:

El objeto del presente contrato específico, derivado del Sistema Dinámico de Adquisición SDA 25/2022, es el suministro de licencias de una solución de arquitectura de ciberseguridad en la nube, para proporcionar un servicio SIEM+SOAR para la prestación del Servicio SOC de SOC para las entidades de la región, en el marco del PRTR cofinanciado por la unión europea-EU, y dentro del proyecto C15.I07.P06 - Programa de Impulso a la Industria de la Ciberseguridad Nacional y la actuación L4-Programa de refuerzo de la estrategia regional de ciberseguridad con la finalidad de garantizar la continuidad del servicio actualmente implantado basado en análisis avanzado y monitorización de amenazas las entidades de la región. Correlacionando eventos, detectando amenazas en tiempo real y automatizando la respuesta ante incidentes, garantizando una protección efectiva de los entornos tecnológicos.

2.2. CARACTERÍSTICAS PRINCIPALES DE LAS PRESTACIONES

Con respecto a las licencias objeto del contrato específico, se admiten programas



- ☒ Puestos a disposición en modalidad de nube.
- ☐ Para su instalación en infraestructura local.
- ☐ En cualquier modalidad de puesta a disposición.

Si están señaladas, las siguientes opciones son de aplicación al presente contrato específico:

- ☒ Se solicita **garantía extendida del adjudicatario** con la cobertura descrita en el apartado III.8 del PPT y concretada en el **Anexo VII** de este documento, cuya duración se extenderá durante todo el periodo de vigencia de las licencias objeto del suministro.
- ☒ Se solicitan **servicios a realizar por el adjudicatario** del contrato específico, para la instalación avanzada o soporte de los suministros. Estos servicios se describen en el **Anexo II**.
- ☒ Se exige el suministro de **soluciones concretas** a fin de garantizar la compatibilidad con las funcionalidades existentes. Se incluye justificación en el **Anexo IV** de este documento.

Con relación a la **definición del número de entregas** la opción señalada es de aplicación al presente contrato específico:

- ☒ El número de unidades a entregar se define con exactitud en este documento de invitación.
- ☐ En el presente contrato el adjudicatario se obliga a entregar una pluralidad de bienes o ejecutar el servicio de forma sucesiva sin que la cuantía total se defina con exactitud en esta invitación por estar subordinada a las necesidades del organismo destinatario.

Definición detallada de las **prestaciones del contrato específico**:

- ☒ Las prescripciones técnicas de los suministros se describen en el **Anexo I**.
- ☒ El contrato requiere servicios de instalación avanzada y/ soporte que se describen en el **Anexo II**.

2.3. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DEL ADJUDICATARIO

El adjudicatario estará sujeto a los términos previstos en la cláusula 27.5.6.2 del PCAP en la ejecución de la prestación, conforme a la opción señalada:

- ☒ **NO. Cláusula aplicable para “Protección de datos sin acceso a datos personales”**. El contrato NO requiere tratamiento de datos personales por parte del adjudicatario.
- ☐ **SÍ. Cláusula aplicable para “Protección de datos con acceso a datos personales”**. El contrato SI requiere tratamiento de datos personales por parte del adjudicatario. La finalidad para la que se ceden los datos es: Haga clic o pulse aquí para escribir texto.

2.4. CATEGORIZACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD (ENS)



☐ El organismo destinatario ha categorizado el sistema o sistemas de información en los que se va a utilizar el programa suministrado, de la siguiente manera:

- Sistema Haga clic o pulse aquí para escribir texto.: categoría Elija un elemento.
- Sistema Haga clic o pulse aquí para escribir texto.: categoría Elija un elemento.
- Haga clic o pulse aquí para escribir texto.

URL donde se publica la certificación o declaración de conformidad (art. 38.2 del ENS): Haga clic o pulse aquí para escribir texto.

☒ No dispone todavía de la categorización del sistema o sistemas de información en los que se va a utilizar el programa.

Relación de los suministros con la arquitectura de seguridad

☐ Los programas **no forman parte de la arquitectura de seguridad**

☒ El suministro incluye programas que **forman parte de la arquitectura de seguridad** del sistema de información resultando de aplicación lo previsto en el **apartado 9.3** del documento de invitación¹. Los programas objeto del presente contrato específico, que forman parte de la arquitectura de seguridad del organismo destinatario son los siguientes²:

Todos los enumerados en el Anexo I de prescripciones técnicas

2.5. TRATAMIENTOS DE DATOS PERSONALES PARA LOS PROGRAMAS EN MODALIDAD DE NUBE

Si el licitador incluye en su oferta **programas puestos a disposición en modalidad nube**:

☒ Los programas objeto del suministro no van a procesar ni almacenar datos de carácter personal, por lo que no existe tratamiento de datos y no son de aplicación ni la Ley Orgánica 3/2018 ni la Ley Orgánica 7/2021. No aplica el apartado 9.4 de este documento de invitación.

☐ Los programas objeto del suministro deben procesar o almacenar datos de carácter personal conforme a lo dispuesto en el **Reglamento (UE) 2016/679**, en adelante RGPD, y en la **Ley Orgánica 3/2018**. Se describen las condiciones aplicables en el apartado 9.4 de este documento de invitación.

☐ Los programas objeto del suministro deben procesar o almacenar datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, conforme a lo dispuesto en la

¹ La arquitectura de seguridad debe estar documentada según [op.pl.2], y al menos uno de los sistemas de información en los que se van a usar dichos programas es de categoría media o alta.

² En la lista de programas de este apartado sólo pueden incluirse los que figuren documentados según [op.pl.2].



Directiva (UE) 2016/680 y la Ley Orgánica 7/2021. Se describen las condiciones aplicables en el apartado 9.4 de este documento de invitación.

Los tratamientos de datos personales en la nube y las finalidades de los tratamientos, así como las medidas que deben aplicarse se definen en el **Anexo III** de este documento.

3. DURACIÓN DEL CONTRATO

3.1. FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

- ☒ Al día siguiente al de adjudicación del contrato.
- ☐ El dd/mm/aaaa, 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 adjudicación del contrato específico.

3.2. PLAZO DE ENTREGA DE LAS LICENCIAS

- ☒ No admite entregas parciales. **Plazo máximo** de entrega³: 30 días naturales contados a partir de la fecha de inicio de ejecución del contrato.
- ☐ Deben realizarse entregas parciales. Los plazos y lugar de las entregas se detallan en el **Anexo VII**.

3.3. PLAZO DE EJECUCIÓN DEL CONTRATO

- ☐ Se requiere la instalación y configuración básica de las licencias, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo⁴ de 30 días hábiles, incluido el plazo de entrega de las licencias.
- ☒ El contrato incluye el servicio de instalación avanzada, a prestar por el adjudicatario, descrito en el **Anexo II** apartado 1. El plazo de ejecución de este servicio incluye el plazo para la entrega de las licencias y para la instalación y configuración básica.
 - Plazo de ejecución: 90 días desde la entrega de las licencias
- ☒ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario, descritos en el **Anexo II**, apartado 2:
 - Plazo de ejecución (señalar únicamente una opción):
 - ☒ 12 meses a contar desde el final de la instalación básica y, en su caso, de la instalación avanzada.

³ Por defecto, 15 días naturales. El organismo podrá indicar un plazo superior.

⁴ Por defecto, 30 días hábiles. El organismo podrá indicar un plazo superior. Este plazo incluye los 15 días naturales para la entrega de las licencias. El cumplimiento del plazo por parte del adjudicatario será exigible cuando el organismo haya puesto a disposición del adjudicatario un entorno limpio en caso de nueva instalación, en un plazo no superior a 20 días hábiles.



☐ Hasta la expiración de la vigencia de las licencias objeto del suministro.

Plazo de ejecución del contrato: consiste en el plazo de entrega de las licencias (incluyendo entregas parciales, en su caso), el plazo de ejecución de la instalación básica (IV.1 del PPT) y el plazo de ejecución de los servicios de instalación avanzada y de soporte descritos.

3.4. 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.

4. VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN

4.1. PRESUPUESTO DE LICITACIÓN Y APLICACIONES PRESUPUESTARIAS

Presupuesto total sin impuestos (€)	Impuestos indirectos (€)	Presupuesto total con impuestos (€)
1.507.620,90 €	316.600,39 €	1.824.221,29 €

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
SUMINISTRO			
Suministro de licencias (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	1.249.785,00 €	262.454,85 €	1.512.239,85 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	149.932,29 €	31.485,78 €	181.418,07 €
Servicio de soporte, a prestar por el adjudicatario	107.903,62 €	22.659,76 €	130.563,37 €
Modificación prevista 20% (Estimación)			
TOTAL	1.507.620,90 €	316.600,39 €	1.824.221,29 €

Si se ha señalado en el apartado 2.2. que las necesidades del contrato no se establecen con exactitud en el documento de invitación, conforme a lo previsto en la disposición adicional trigésima tercera de la LCSP, este presupuesto será estimado y no obligatorio para la entidad, y supondrá el importe máximo del contrato específico.

En todo caso, el importe de los servicios deberá ser inferior al importe de los suministros. Asimismo, cada uno de los conceptos presupuestarios desglosados en la tabla anterior (suministro de licencias, instalación avanzada y/o soporte) opera como límite máximo de gasto, por lo que las ofertas no deberán superar el importe de ninguno de ellos, incluso aunque el importe total de la oferta en su conjunto sea inferior al presupuesto base de licitación. Serán excluidas del procedimiento las ofertas que no se adecuen a estas estipulaciones.

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, Centro de Gestión Agencia de Ciberseguridad de la Comunidad de Madrid, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	Anualidad 2026	Anualidad 2027	TOTAL
Suministro de Licenciamiento de software para una solución SIEM SOAR-SOC de SOC's para las entidades de la región	1.758.939,61 €	65.281,69 €	1.824.221,29 €

La licitación se co-financia principalmente con fondos MRR RETECH y Fondos Propios de la Agencia de Ciberseguridad con el siguiente reparto.

Cofinanciado	Fondos	Anualidad 2026	Anualidad 2027	Total
<i>Fondos RETECH</i>	92,84%	1.399.717,29 €		1.399.717,29 €
<i>Fondos Propios</i>	7,16%	53.951,81 €	53.951,81 €	107.903,62 €
IVA		305.270,51 €	11.329,88 €	316.600,39 €
		1.758.939,61 €	65.281,69 €	1.824.221,29 €

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

4.2. DETERMINACIÓN DEL PRECIO DEL CONTRATO

De acuerdo con los artículos 102.4 y 309 del LCSP, la determinación del precio del contrato se realiza a tanto alzado.

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	96.342,51 €
Resto costes directos	1.249.747,58 €
Costes indirectos + Gastos generales + Beneficio industrial	161.530,81 €
Total sin IVA	1.507.620,90 €

Justificación: El objeto del contrato incluye la adquisición de licencias de software y servicios adicionales de soporte personalizado. Los costes directos abarcan ambos conceptos, más un 6% de gastos generales y un 6% de beneficio industrial.



Dado que se solicitan servicios, el valor estimado incorpora los costes laborales según el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública (BOE 16/04/2025, Resolución de 4/04/2025 de la Dirección General de Trabajo). No existen diferencias por género en el convenio.

Costes de personal							
Perfiles	Dedicación	Salario Base	Especialización tecnológica (XX%) ⁵	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 30%
Jefe de proyecto	10%	35.674,43 €	100%	35.674,43 €	3.567,44 €	3.567,44 €	4.709,02 €
Analista SOC L1/L2 (Monitoreo y Alertas)	100%	23.375,89 €	100%	23.375,89 €	23.375,89 €	23.375,89 €	30.856,17 €
Analista SOC L2 (Automatización y SOAR)	100%	23.375,89 €	100%	46.751,78 €	46.751,78 €	46.751,78 €	60.777,31 €
							96.342,51 €

Los servicios asociados al contrato tienen carácter accesorio e instrumental respecto del suministro de licencias, que constituye el objeto principal del contrato. La inclusión de costes de personal responde exclusivamente a la necesidad de prestar los servicios accesorios de instalación avanzada y soporte, sin alterar la naturaleza del contrato como contrato de suministro.

Si bien resulta de aplicación el convenio colectivo sectorial, la ejecución de dichos servicios requiere una cualificación superior, derivada de la especialización tecnológica exigida y del limitado número de recursos disponibles en el mercado en el ámbito de la ciberseguridad. A estos efectos, la estimación de los costes de personal se ha realizado tomando como referencia los salarios de mercado y el informe de la consultora Hays 2025, correspondiente al Área 5 de Ciberseguridad, aplicándose los coeficientes de especialización tecnológica reflejados en la tabla anterior.

4.3. TRAMITACIÓN DEL EXPEDIENTE (A EFECTOS PRESUPUESTARIOS)

☒ Ordinaria.

☐ Anticipada:

Se hace constar que el plazo de ejecución comenzará a partir del **1 de enero de 202X o fecha posterior**, 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.

⁵ Se requiere personal con conocimientos, habilidades y destrezas específicos que conlleven que el personal que posee dichas competencias técnicas esté especialmente reconocido y valorado en el mercado laboral. (Importante: en caso de incluir este porcentaje de especialización tecnológica, el organismo deberá justificarlo o indicar el origen de la estimación realizada).



4.4. MODIFICACIÓN DEL CONTRATO ESPECÍFICO

☒ **No se prevén modificaciones convencionales** del contrato, todo ello sin perjuicio de los supuestos de modificación legal contemplados en el artículo 205 de la LCSP.

☐ El contrato específico **podrá ser modificado** durante su vigencia, conforme a lo previsto en los artículos 203.a) y 204 LCSP, en un porcentaje máximo del 20% del precio inicial de adjudicación.

Serán de aplicación las siguientes condiciones:

No aplica

- Circunstancias admitidas para modificar el contrato específico⁶:
 - No aplica

Si el contrato específico **está financiado por el PRTR**, adicionalmente a lo anterior es de aplicación la Cláusula Adicional Tercera, de modificación de los contratos específicos financiados en el PRTR, incluida en la Adenda a este documento de invitación.

4.5. VALOR ESTIMADO

Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **UN MILLÓN QUINIENTOS SIETE MIL SEISCIENTOS VEINTE EUROS CON NOVENTA CÉNTIMOS euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	1.507.620,90€
Importe máximo por modificación prevista, sin IVA	Haga clic o pulse aquí para escribir texto.
TOTAL	1.507.620,90€

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

☒ **SI** está sujeto a regulación armonizada

☐ **NO** está sujeto a regulación armonizada

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

☐ No.

☒ Sí. Instrumento /Fondo/Programa/Mecanismo: C15.I07.P06.S61

⁶ Entre las circunstancias que se pueden señalar deben precisarse las admitidas en el apartado 27.17 del PCAP del SDA 25/2022.



Código de operación/Proyecto/Iniciativa: C15.I07.P06.S61.SI01.PROVISIONAL.04

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 con cargo al presupuesto de la Unión Europea.

5. LUGAR Y CONDICIONES DE LA ENTREGA

Los **datos de la entrega** de los suministros, en caso de no coincidir con los datos del organismo interesado, son:

- Dirección Postal: Haga clic o pulse aquí para escribir texto.
- Correo electrónico: Haga clic o pulse aquí para escribir texto.
- Teléfono: Haga clic o pulse aquí para escribir texto.
- Fax: Haga clic o pulse aquí para escribir texto.

En caso de haberse indicado en el apartado 2 que se admiten entregas parciales, el lugar de entrega para cada entrega parcial será el indicado en el **Anexo VII**.

El responsable del contrato específico podrá determinar para la entrega y/o recepción de los suministros un lugar distinto al aquí indicado, previa aceptación y conformidad del adjudicatario del contrato.

6. INCOMPATIBILIDADES PARA LA LICITACIÓN

☒ **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 a realizar por el adjudicatario.

☐ **Sí han participado empresas** en la elaboración de especificaciones técnicas o de los documentos preparatorios del contrato específico. 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:
(*Detallar en su caso*)

☐ Existen incompatibilidades por causa de la naturaleza de los trabajos.
(*Determinar la incompatibilidad existente y justificar*)



7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN⁷

7.1. PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN

- ☐ El único criterio de adjudicación es el precio
- ☐ Solo se utiliza el precio y otros criterios evaluables mediante fórmulas, con los siguientes pesos:

SOBRE 1.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 1.2. Precio
N/A.	N/A

- ☒ Conforme a lo justificado en memoria adjunta, se utilizan criterios sujetos a un juicio de valor con los siguientes porcentajes:

SOBRE 1. Criterios que dependen de un juicio de valor	SOBRE 2.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 2.2. Precio
25	35	40

7.2. FÓRMULA APLICABLE AL CRITERIO PRECIO

- ☒ Función **optimizar precio** (si se incluyen criterios cuya cuantificación depende de un juicio de valor, se deberá usar ésta obligatoriamente):

$$C_i = P * \frac{O_l - O_i}{O_l - O_b}$$

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.

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

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

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

- ☐ Función **minimizar precio** (se puede utilizar si sólo se utilizan criterios automáticos):

$$C_i = P * \left(1 - \frac{O_i - O_{min}}{O_{max}} \right)$$

Donde:

⁷ Criterios de valoración conforme a las previsiones del apartado 27.5.4 del PCAP.



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.
 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)

7.3. OTROS CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS, DISTINTOS AL PRECIO

7.3.1. CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS

Los criterios técnicos recogidos en la tabla siguiente serán evaluados de forma automática y objetiva, aplicando las fórmulas indicadas conforme al apartado 7.3.2 de este documento. La puntuación máxima total de este bloque será de **35 puntos**.

COD	CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓN, según apartado 7.5
B.1	Arquitectura nativa en nube pública	4	Función maximizar
B.2	Modelo de datos inmutable y optimizado	3	Función maximizar
B.3	Capacidad de ingestión y conectividad nativa	2	Función maximizar
B.4	Integración nativa SIEM–SOAR e Inteligencia de Amenazas	6	Función maximizar
B.5	Motor de automatización sin código	5	Función maximizar
B.6	Detección mediante IA y aprendizaje automático	2	Función maximizar
B.7	Playbooks automatizados	2	Función Minimizar
B.8	Soporte multi-entidad y aislamiento lógico	3	Función maximizar
B.9	APIs abiertas y SDK de integración	2	Función maximizar
B.10	Servicios Asociados	6	Función maximizar

Estos criterios se centran exclusivamente en aspectos diferenciales y objetivos que aportan valor añadido al servicio y que no coinciden con los requisitos mínimos establecidos en el Anexo I.

A continuación, se establecen definiciones precisas de cada criterio, incluyendo evidencias mínimas exigibles, con el fin de asegurar una valoración homogénea y verificable.

B1.-Arquitectura nativa en nube pública

La plataforma deberá ser un servicio totalmente gestionado (SaaS), desplegado en infraestructura nativa de nube pública, con capacidad de escalar horizontalmente sin limitación y procesar más de 100 TB/día sin degradación del rendimiento.

Las ofertas deberán de indicar Ofertas indicarán: **Capacidad ingestión máxima (TB/día)**

B2.-Modelo de datos inmutable y optimizado

Se valorará que el modelo de datos sea inmutable, basado en almacenamiento columnar y optimizado para consultas masivas sobre datos estructurados y no estructurados.



Las ofertas deberán de indicar Ofertas indicarán: **Periodo mínimo de retención garantizada en meses**

B3.-Capacidad de ingestión y conectividad nativa

El sistema deberá permitir la ingestión de datos en tiempo real desde más de 300 fuentes heterogéneas sin uso de agentes, utilizando conectores nativos o APIs estandarizadas.

Las ofertas deberán de indicar Ofertas indicarán: **Nº conectores nativos disponibles**

B4.- Integración nativa SIEM–SOAR e Inteligencia de Amenazas

Se valorará la integración completa entre SIEM, SOAR e Inteligencia de Amenazas en una única consola, permitiendo la gestión de alertas, casos y flujos automatizados sin herramientas externas.

Las ofertas deberán de indicar Ofertas indicarán: **Nº componentes integrados nativamente (máx.5)**

B5.-Motor de automatización sin código

El sistema deberá incorporar un motor de orquestación visual que no requiera programación, con flujos reutilizables y parametrizables. Valorándose la posibilidad de redactar playbooks en lenguaje natural en castellano.

Las ofertas deberán de indicar Ofertas indicarán: **Nº playbooks predefinidos reutilizables**

B6.-Detección mediante IA y aprendizaje automático

Se valorará la existencia de capacidades de detección autónoma basadas en inteligencia artificial, capaces de identificar comportamientos anómalos sin etiquetado previo.

Las ofertas deberán de indicar Ofertas indicarán: **% alertas generadas por IA/ML**

B7.-Playbooks automatizados

La solución proporcionará un conjunto de reglas y playbooks, con el objetivo de reducir los tiempos de respuesta ante incidentes.

Las ofertas deberán de indicar Ofertas indicarán: **promedio de ejecución playbook en segundos**

B8.-Soporte multi-entidad y aislamiento lógico

Se valorará que el sistema permita la gestión de múltiples entidades dentro de una única plataforma, garantizando segregación lógica, políticas y dashboards independientes.

Las ofertas deberán de indicar Ofertas indicarán: **Nº tenants simultáneos soportados**

B9.-APIs abiertas y SDK de integración

Se valorará la disponibilidad de APIs REST y SDK documentados para integración con sistemas externos (ticketing, CMDB, vulnerabilidades, etc.).

Las ofertas deberán de indicar Ofertas indicarán: **Nº despliegues SOC últimos 3 años**

B10.-Servicios Asociados

Se valorará la calidad de los servicios asociados y su adecuación a las necesidades del SOC de SOC's.

Las ofertas deberán de indicar Ofertas indicarán: **Nº endpoints REST documentados**

7.3.2. FÓRMULAS PARA LA EVALUACIÓN AUTOMÁTICA DE LOS CRITERIOS



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 saciedad 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:

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

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.

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

Los criterios incluidos en esta sección serán valorados mediante un juicio de valor técnico, conforme a los aspectos detallados en el apartado 7.4.2. La puntuación máxima total de este bloque será de **25 puntos**.

La documentación relativa a estos criterios deberá incluirse exclusivamente en la oferta técnica correspondiente al Sobre nº 1.

Para preservar la objetividad y evitar solapamientos con los criterios evaluables automáticamente (Sobre nº 2), los criterios sujetos a juicio de valor valoran el enfoque técnico, arquitectura y madurez de la solución, **sin referencia a métricas, umbrales o valores cuantificables**, que serán objeto exclusivo de los criterios evaluables automáticamente, en el Sobre nº 1 está expresamente prohibido:

- Cualquier referencia, dato o descripción que permita
 - identificar/inferir cumplimiento de criterios obligatorios SÍ/NO del Sobre 2.1 (ej. arquitectura nativa, motor sin código).



- Mención directa/indirecta a requisitos "debe" (nombres soluciones, capturas APIs, etc.).
- Anexos/enlaces que acrediten obligaciones del Sobre 2 antes de su evaluación.

El incumplimiento podrá conllevar la desestimación de la oferta si la mesa lo considera procedente.

Cuando sea imprescindible justificar una capacidad, el licitador deberá hacerlo sin revelar cuantías, describiendo procedimientos, flujos, controles, perfiles, pantallas genéricas y políticas (no métricas ni inventarios).

7.4.1. CRITERIOS Y PONDERACIÓN

	CRITERIO Ponderación Máxima: Puntos	PUNTOS Máximos
A1	Almacenamiento de 12 meses en caliente	5
A2	Cumplimiento ENS Alto y certificaciones internacionales	4
A3	Normalización automática y modelo de datos unificado	3
A4	Correlación del alto rendimiento	3
A5	Cuadros de mando analíticos sobre la misma tecnología de datos	10

7.4.2. MÉTODO DE VALORACIÓN Y DOCUMENTACIÓN

A1.-Almacenamiento de 12 meses en caliente

Se valorará que el sistema permita ejecutar consultas sobre cualquier capa de datos sin recuperación de datos archivados, con independencia del volumen y antigüedad de al menos 12 meses.

A2.-Cumplimiento ENS Alto y certificaciones internacionales

Se valorará el cumplimiento con ENS (categoría Alta), ISO/IEC 27001, tanto en la infraestructura como en el servicio ofertado. Incluido en catálogo CCN-STIC-105.

A3.-Normalización automática y modelo de datos unificado

Se valorará la capacidad de la plataforma para aplicar automáticamente un modelo de datos común y normalizado a todas las fuentes de información, mejorando la correlación entre orígenes.

A4.-Correlación del alto rendimiento

El sistema deberá ejecutar búsquedas con latencia de pocos segundos sobre un histórico de un año.

A5.-Cuadros de mando analíticos sobre la misma tecnología de datos

El licitador deberá ofrecer un entorno analítico para el desarrollo de dashboards basados directamente en la misma tecnología de procesamiento que el SIEM, con integración directa y sin duplicación de datos. El sistema deberá admitir la integración de fuentes heterogéneas, como datos en formato CSV o imagen.



El baremo de la valoración cualitativa, para cada uno de los criterios, es:

10 Puntos - Excelente: Cumple de forma sobresaliente todos los requisitos, con capacidades nativas superiores a lo exigido y características técnicas diferenciadoras acreditadas documentalmente.

8 Puntos - Muy Bueno: Cumple completamente todos los requisitos con solución nativa integrada, sin requerir desarrollos adicionales significativos.

5 Puntos - Adecuado: Cumple los requisitos mínimos mediante integración de componentes externos o configuraciones complejas, con limitaciones técnicas documentadas.

2 Puntos - Básico: Cumple requisitos mínimos con soluciones alternativas que requieren desarrollos extensivos o comprometen rendimiento.

0 Puntos - Inadecuado: No acredita cumplimiento de requisitos mínimos o solución propuesta inviable técnicamente.

Cada criterio se puntúa:

$$P_{\text{final}} = P_{\text{máx}} \times \text{factor baremo (redondeo aritmético)}.$$

Se aplicará un umbral del 50% una vez abierto el Sobre nº 1 y, si existen también criterios de calidad automáticos, una vez abierto también el sobre 2.1.

8. OFERTAS ANORMALMENTE BAJAS

Se apreciará que la oferta es anormalmente baja 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 anterior, siempre que existan criterios diferentes al precio, se deberá añadir la siguiente para apreciar el carácter anormal o desproporcionado de las ofertas.
 - ☐ Cuando la puntuación en el criterio de calidad de mayor peso de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media de los valores ofertados: *indicar % o importe*.



☒ Cuando la puntuación conjunta de todos los criterios de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media la puntuación de todas las ofertas en estos criterios: **20 %**.

Haga clic o pulse aquí para escribir texto.

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) A ofertar únicamente programas con distribución comercial, no pudiendo aplicar precios superiores a los de mercado conforme a las condiciones del apartado 17.2 c) del PCAP, y que satisfagan las prestaciones de la garantía obligatoria del fabricante previstas en el apartado III.6 del PPT.
- b) La obligación de cumplimiento de la condición especial de ejecución relativa a la disponibilidad de los planes de formación conforme al apartado 27.5.6 apartado 1 del PCAP y, en su caso, las condiciones de ejecución previstas en el apartado 9.3 de este documento de invitación.
- c) Las obligaciones referidas a la protección de datos personales, en los términos previstos en la cláusula 27.5.6 apartado 2 del PCAP.
- d) La obligación de confidencialidad del apartado 27.5.8 del PCAP.
- e) Las obligaciones establecidas en el apartado 27.5.9 del PCAP respecto al personal laboral.
- f) A facilitar la información técnica prevista en los apartados III.9 y III.10 del PPT de los productos ofertados, en caso de resultar adjudicatario.
- g) 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 artículo 215.2.e) de la LCSP, el contratista principal no podrá subcontratar las siguientes tareas críticas:

(Indicar, si las hay, las tareas críticas que no pueden ser subcontratadas):

- *Tarea crítica 1*
- *Tarea crítica 2*
- ...

- h) Si el contrato incluye servicios a prestar por el adjudicatario, estará obligado al cumplimiento de las condiciones salariales de los trabajadores conforme al convenio colectivo sectorial de aplicación conforme al artículo 122.2 de la LCSP.
- i) 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 la prestación por parte de la empresa adjudicataria.

9.2. OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO



El Documento de Invitación del SDA 25/2022 responde a un modelo normalizado y cerrado, sin posibilidad técnica de incorporar texto explicativo en los apartados 2.3 y 2.5.

Sin perjuicio de que, conforme a estos apartados, el objeto principal del contrato no implique tratamiento de datos personales en sentido estricto, la naturaleza de las soluciones de ciberseguridad objeto del presente contrato puede conllevar el tratamiento incidental de metadatos técnicos, identificadores indirectos o información asociada a eventos de seguridad. En consecuencia, y con carácter preventivo, durante la ejecución del contrato resultarán de aplicación las obligaciones en materia de protección de datos personales previstas en este documento y en la normativa vigente.

Por este motivo, y sin contradecir las opciones marcadas ni modificar el objeto del contrato, la aclaración correspondiente se incorpora en el apartado 9.2, único apartado del modelo que admite texto libre.

Dicha inclusión tiene carácter aclaratorio y preventivo, sin implicar la existencia de un tratamiento de datos personales como prestación principal.

9.3. OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

A efectos del artículo 11 del RD 311/2022, en adelante ENS, el responsable del sistema, será el que se indique en este documento de invitación o, en caso de no indicarse explícitamente, el responsable del sistema será el responsable del contrato específico que figura en el apartado 1 del presente documento.

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 requisitos de seguridad exigidos en esta cláusula y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes de seguridad durante la ejecución del contrato específico. 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.

En caso de que el contrato específico incluya la prestación de servicios por parte del adjudicatario, 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 para la prestación del citado servicio, en cumplimiento del artículo 15 del ENS. Esta información se realizará en la fase de 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.

Si alguno de los sistemas de información en los que se van a utilizar los programas en infraestructura local es de categoría media o alta, el adjudicatario del contrato específico debe proporcionar al Responsable del Contrato Específico durante la ejecución del contrato la lista de componentes software, en cumplimiento de la medida [op.pl.5.r2.1] del ENS.

9.4. OBLIGACIONES RELATIVAS AL CUMPLIMIENTO DE LAS CONDICIONES DE LOS PROGRAMAS OFERTADOS EN MODALIDAD DE NUBE CUANDO EXISTA TRATAMIENTO DE DATOS PERSONALES



A los efectos del Reglamento (UE) 2016/679, el proveedor de nube tendrá consideración de encargado del tratamiento.

Si se ha indicado en el apartado 2.2 que los programas objeto del suministro deben procesar o almacenar datos de carácter personal conforme a lo dispuesto en el **Reglamento (UE) 2016/679**, en adelante RGPD, y en la **Ley Orgánica 3/2018**, o tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, conforme a lo dispuesto en la **Directiva (UE) 2016/680** y la **Ley Orgánica 7/2021**, sólo se aceptarán nubes cuyos proveedores de nube encargados del tratamiento se encuentren establecidos y realicen las operaciones principales de tratamiento en la UE/EEE, admitiéndose transferencias a terceros países u organizaciones internacionales siempre que el proveedor de nube establecido en la UE/EEE ofrezca garantías adecuadas conforme a lo previsto en el Capítulo V del RGPD⁸.

El candidato propuesto como mejor clasificado deberá acreditar que el **proveedor de nube** está en disposición de suscribir el acto jurídico vinculante de conformidad al artículo 28.3 del Reglamento (UE) 2016/679 (RGPD) durante el período de vigencia de las licencias en su condición de encargado del tratamiento. A estos efectos, el licitador mejor clasificado deberá aportar la declaración responsable que figura en el **Anexo V** y que debe incluir información suficiente del proveedor de nube de los suministros. El responsable del tratamiento, a la vista de la documentación, manifestará su conformidad en el modelo del **Anexo VI**.

En caso de no aportarse la declaración responsable y la documentación del proveedor de nube en un plazo máximo de cinco días hábiles, o de que las garantías ofrecidas por el proveedor de nube no sean suficientes, la oferta podrá ser excluida, en cuyo caso se procederá a recabar la misma documentación al licitador siguiente, por el orden en que hayan quedado clasificadas las ofertas.

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

Se abonará el precio del **suministro de las licencias** dentro de los treinta días siguientes a la fecha de aprobación de las certificaciones (parciales o totales, según se indique en el apartado 3.2 de este documento de invitación) o de los documentos que acrediten la conformidad con lo dispuesto en el contrato de los bienes entregados, conforme a las previsiones del art. 198.4 del LCSP.

Si en el apartado 2.2 y 3.3 se ha indicado que se solicita un **servicio de instalación avanzada** a prestar por el adjudicatario, éste se facturará:

- ☒ A la recepción del servicio, tras su cumplimiento a satisfacción de la Administración.
- ☐ Otra: Haga clic o pulse aquí para escribir texto.

⁸ La Comisión Europea ha adoptado decisiones de adecuación con Andorra, Argentina, Canadá (operaciones comerciales sólo), Islas Faroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, República de Corea, Suiza, Reino Unido y Uruguay. Puede obtenerse información adicional actualizada en la página de la AEPD <https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales>.



Si en el apartado 2.2 y 3.3 se ha indicado que se solicita un **servicio de soporte** a prestar por el adjudicatario, éste se facturará:

- ☒ Mensualmente.
- ☐ Trimestralmente, considerando los siguientes períodos trimestrales:
- Período 1: Haga clic o pulse aquí para escribir texto.
- Período 2: Haga clic o pulse aquí para escribir texto.
- Período 3: Haga clic o pulse aquí para escribir texto.
- Período 4: Haga clic o pulse aquí para escribir texto.
- ☐ Otra: Especificar...

10.2. 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 (XAES).

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 (DIR3): Haga clic o pulse aquí para escribir texto.
- Órgano gestor (DIR3): Haga clic o pulse aquí para escribir texto.
- Unidad tramitadora (DIR3): Haga clic o pulse aquí para escribir texto.
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3): Haga clic o pulse aquí para escribir texto.

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

- Campo <FileReference>: SDA 25/2022.
- Campo <Receiver transaction reference>: código del contrato específico.

- ☒ Organismo adherido al Sistema Estatal de Contratación Centralizada.

La Agencia de Ciberseguridad de la Comunidad de Madrid gestionará, 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 en el campo ReceiverTransactionReference el valor ACR-009-2026.



11. GARANTÍA DE LOS BIENES

Una vez efectuada la recepción de las licencias de los programas suministradas, comenzará el plazo de garantía de según lo establecido en los artículos 210 y 305 de la LCSP.

Esta garantía, denominada **garantía obligatoria del adjudicatario**, se ajustará a lo descrito en el apartado III.7 del PPT y tendrá una duración de 2 años independientemente del periodo de vigencia de las licencias suministradas.

En caso de haberse solicitado en el apartado 2.2, a la anterior garantía obligatoria del adjudicatario, será obligatoria una **garantía extendida del adjudicatario** con la cobertura del apartado III.8 del PPT, concretada en el **Anexo VIII** de este documento, cuya duración se extenderá durante todo el periodo de vigencia de las licencias objeto del suministro.

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

En los siguientes casos se aplicarán las previsiones de la cláusula 27.16 del PCAP:

	Valor fijado en el SDA	Valor fijado en el contrato específico	Fórmula de cálculo
Incumplimiento de las condiciones especiales de ejecución, excepto las relativas a subcontratación.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo	<i>No Aplica</i>	N/A
Incumplimiento de los compromisos de adscripción de medios.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Demora en el cumplimiento del plazo total del contrato	Resolución / 0,60 euros por cada día y 1.000 euros del precio del contrato, IVA excluido		Valor fijado en el SDA



Incumplimiento de obligaciones en materia medioambiental, social o laboral	2% de la facturación del periodo	Apartado 12.2
Incumplimiento de las condiciones de subcontratación	2% del importe del subcontrato	Valor fijado en el SDA
Incumplimiento de las obligaciones de información y pago sobre suministradores y subcontratistas.	2% del importe del subcontrato	Valor fijado en el SDA

Definición y motivación de incumplimientos graves y muy graves aplicables al contrato específico:

- El incumplimiento de las medidas relativas a la seguridad de los programas en cumplimiento del ENS, o de los requisitos de seguridad para la protección de datos personales en nube tendrá la consideración de incumplimiento **muy grave** dando lugar a una penalidad de hasta el **10% del importe total del contrato**.

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:

$$I_p = 0.02 \times I_F \frac{d}{D}$$

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 DEL CONTRATO ESPECÍFICO

Son de aplicación las causas de resolución previstas en el apartado 27.18 del PCAP del sistema dinámico de adquisición.

Haga clic o pulse aquí para escribir texto.

14. FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

Las ofertas se presentarán obligatoriamente en formato electrónico, a través de la PLACSP⁹ u otra plataforma de contratación a disposición del organismo.

Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa¹⁰.

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.

El documento, único, que se incluye en este sobre (OFERTA TÉCNICA), deberá tener una extensión máxima de 25 páginas, con un tamaño de letra mínimo de 10 puntos e interlineado sencillo. Toda oferta técnica que incumpla las características anteriores no será objeto de valoración. La estructura de secciones del documento debe permitir una fácil identificación de los contenidos que responden a los criterios de adjudicación que dependen de un juicio de valor (apartado 7.4).

- **Sobre 2:**

- 2.1: Documentación relativa a los criterios automáticos evaluables mediante fórmulas, distintos del precio. Se deberá presentar esta documentación utilizando la siguiente tabla:

Criterios automáticos evaluables mediante fórmula, distintos del precio	
Arquitectura nativa en nube pública	__VALOR__
Modelo de datos inmutable y optimizado	__VALOR__
Capacidad de ingestión y conectividad nativa	__VALOR__
Integración nativa SIEM–SOAR e Inteligencia de Amenazas	__VALOR__
Motor de automatización sin código	__VALOR__
Detección mediante IA y aprendizaje automático	__VALOR__
Playbooks automatizados	__VALOR__

⁹ Plataforma de Contratación del Sector Público:
<https://contrataciondelestado.es/wps/portal/quiasAyuda>

¹⁰ Para facilitar la identificación el firmante apoderado de la empresa se deberá indicar, además de sus datos, el número de usuario apoderado de la aplicación AUNA.



Criterios automáticos evaluables mediante fórmula, distintos del precio	
Soporte multi-entidad y aislamiento lógico	__ VALOR __
APIs abiertas y SDK de integración	__ VALOR __
Servicios Asociados	__ VALOR __

- 2.2: Oferta económica: **deberá incluir el desglose de los importes** correspondientes según los conceptos presupuestarios indicados en la tabla de detalle del presupuesto de licitación del apartado 4.1., para lo cual se deberá utilizar el modelo de oferta disponible en el Portal de Contratación Centralizada, para el SDA 25/2022, en la siguiente dirección:
https://contratacioncentralizada.gob.es/documents/32143/48667/Modelos+de+Oferta+SDA25_2022.zip/b255fa33-a721-b657-d308-743f00fb56b4?t=1759159939180

En el supuesto de que se hayan definido criterios sujetos a juicio de valor, se deberá incluir en el Sobre 1 de la oferta técnica, la documentación que permita evaluar los planes de implantación o las soluciones técnicas conforme a los criterios sujetos a un juicio de valor, sin que sea posible incluir en este sobre información económica o correspondiente a criterios automáticos que se presentará en el Sobre 2. El Sobre 1 se deberá valorar de forma previa a la apertura del sobre que contiene la documentación económica y de los criterios evaluables mediante fórmulas.

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 de 3 días naturales a contar desde el día siguiente de la recepción de la invitación a participar en la licitación.

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 suministro de software de sistema, de desarrollo y de aplicación (SDA 25/2022), los pliegos rectores del SDA se encuentran disponibles en el siguiente enlace: https://contrataciondelestado.es/wps/wcm/connect/2e5cb41d-d508-4a7f-ae25-c5f986492db9/DOC_CD2022-214850.pdf?MOD=AJPERES

NOTAS IMPORTANTES: LOS CANDIDATOS ADMITIDOS AL SISTEMA DINÁMICO NO ESTÁN OBLIGADOS A PRESENTAR OFERTA NI A COMUNICAR QUE NO VAN A CONCURRIR A LA LICITACIÓN.

EN LO QUE ESTE DOCUMENTO DE INVITACIÓN SE OPONGA A LOS PLIEGOS DEL SISTEMA DINÁMICO DE ADQUISICIÓN, PREVALECEÁN 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 (CARGO): Consejero Delegado de La Agencia de Ciberseguridad de la Comunidad de Madrid

Firmado electrónicamente (nombre y apellidos): **Alejandro Las Heras Vázquez**



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

Se requiere la adquisición de una solución de ciberseguridad basada en la nube para la ingesta, normalización, correlación y análisis de eventos y datos de seguridad provenientes de diversas fuentes, tanto de infraestructuras públicas como privadas, durante 2 años. El objetivo es optimizar la gestión de la seguridad, acelerar la detección y respuesta ante incidentes, y fortalecer la capacidad de investigación frente a amenazas emergentes mediante un enfoque basado en inteligencia de amenazas integrada, análisis de comportamiento de usuarios y entidades (UEBA), automatización de la respuesta (SOAR) y capacidades avanzadas de IA Agéntica aplicadas a la operación del centro de operaciones de seguridad (SOC).

A continuación, se detallan los requerimientos técnicos del suministro:

Referencia	Programa	Cantidad
Google Security Operations Enterprise Plus EU Subscription, o Equivalente.	Subscriptions/LogIngestBytes/Enterprise Plus/Europe – PrePay. Bytes of data ingested in EU for the Enterprise Plus package o equivalente.	300 GB/day

1. ARQUITECTURA

Arquitectura nativa en la nube pública

La plataforma deberá estar diseñada y desplegada sobre una arquitectura nativa en la nube pública, concebida para ofrecer escalabilidad horizontal prácticamente ilimitada. Dicha arquitectura deberá permitir el procesamiento simultáneo de grandes volúmenes de información en tiempo real sin degradar el rendimiento, incluso en escenarios de alta concurrencia o crecimiento rápido de entidades conectadas. El sistema deberá ser capaz de adaptarse dinámicamente a la demanda de recursos, incrementando o reduciendo su capacidad de cómputo de forma automática, sin requerir tareas de aprovisionamiento manual ni intervención del adjudicatario o del personal técnico de la Administración. Este modelo de servicio garantizará la continuidad operativa, la resiliencia frente a fallos y la disponibilidad permanente de la información procesada.

Modelo de datos inmutable y almacenamiento columnar

El modelo de datos subyacente deberá ser inmutable, garantizando que toda la información registrada mantenga su integridad y trazabilidad a lo largo del tiempo. La solución deberá emplear un sistema de almacenamiento columnar distribuido, optimizado para búsquedas analíticas masivas, correlaciones complejas y procesamiento paralelo. Este enfoque permitirá indexar grandes volúmenes de registros de seguridad sin pérdida de velocidad, minimizando los tiempos de respuesta en consultas históricas o de carácter forense. El modelo columnar proporcionará un



rendimiento homogéneo tanto para datos recientes como para históricos, asegurando que las operaciones de detección y análisis se realicen con máxima eficiencia.

Almacenamiento de datos de al menos 12 meses

La arquitectura deberá establecer una separación clara entre las capas de ingestión, almacenamiento y análisis, de forma que cada componente del sistema pueda escalar de manera independiente según su carga de trabajo. Esta segmentación funcional permitirá realizar consultas directamente sobre datos de al menos 12 meses, sin necesidad de procesos de recuperación, reconstrucción o migración entre niveles de almacenamiento. El modelo garantizará que la plataforma mantenga su rendimiento independientemente de la antigüedad o volumen de los datos consultados, optimizando el uso de los recursos y reduciendo los costes operativos.

Modelo SaaS gestionado por el fabricante

El servicio deberá ofrecerse bajo un modelo completamente gestionado (Software as a Service, SaaS), en el que la infraestructura subyacente, las actualizaciones, la escalabilidad y las tareas de mantenimiento sean responsabilidad exclusiva del fabricante de la solución. El adjudicatario no deberá gestionar servidores, máquinas virtuales, bases de datos ni servicios de red asociados. Este modelo permitirá a la Administración centrar sus recursos en la operación de seguridad y en la explotación de la información, garantizando además un ciclo de actualización continuo, sin interrupciones ni riesgo de obsolescencia tecnológica.

2. CAPACIDAD DE INGESTIÓN Y NORMALIZACIÓN

Ingestión en tiempo real y conectores nativos

La plataforma deberá ser capaz de ingerir datos en tiempo real desde un número superior a 300 fuentes distintas, sin la necesidad de desplegar agentes dedicados en los sistemas de origen. Para ello, deberá disponer de conectores nativos y bibliotecas predefinidas que faciliten la integración con infraestructuras corporativas, dispositivos de red, aplicaciones en la nube y sistemas industriales. Esta capacidad garantizará la fluidez y coherencia en la transmisión de información, así como la reducción del tiempo necesario para incorporar nuevas fuentes de datos al sistema.

Normalización de eventos en modelo de datos unificado

El sistema deberá implementar un modelo de datos unificado que permita normalizar automáticamente los eventos procedentes de diferentes tecnologías, fabricantes o entornos. Esta normalización será clave para la correlación avanzada y la detección contextual de incidentes. Los datos recolectados deberán almacenarse siguiendo una estructura coherente y extensible, que facilite la búsqueda y comparación entre entidades, además de permitir la aplicación de reglas y políticas de detección de forma homogénea en todo el entorno.

Motor de búsqueda y correlación de alto rendimiento

La plataforma deberá incluir un motor de búsqueda y correlación basado en lenguaje estándar de consulta, capaz de ejecutar consultas complejas sobre volúmenes masivos



de información con latencia inferior a tres segundos, incluso al trabajar sobre un histórico de datos de al menos un año (para lo que dispondrá de dicha información en caliente). Este motor deberá permitir la exploración instantánea de registros para labores de investigación forense, respuesta a incidentes o auditoría, sin requerir procesos previos de indexado o particionado de datos.

3. DETECCIÓN, ANÁLISIS Y RESPUESTA (SOAR)

Integración nativa SIEM-SOAR

La solución deberá integrar de forma nativa las funcionalidades de monitorización, correlación y orquestación (SIEM y SOAR) dentro de una única interfaz de gestión. Esta integración permitirá la coordinación centralizada de alertas, casos e incidentes, manteniendo una trazabilidad completa de las acciones realizadas y de los estados de cada evento. El operador podrá visualizar el ciclo de vida completo de un incidente, desde su detección inicial hasta su cierre, sin necesidad de herramientas adicionales ni pasos manuales de transferencia de información.

Motor de automatización sin necesidad de código

El sistema deberá incorporar un motor de automatización visual que no requiera conocimientos de programación. Dicho motor deberá permitir la creación de flujos de trabajo reutilizables y personalizables, ajustados al tipo de incidente o a las políticas del SOC. Los playbooks deberán contemplar la ejecución de tareas automáticas y semiautomáticas de análisis, validación, notificación o contención, garantizando una respuesta homogénea y documentada ante cada escenario de amenaza. Dichos playbooks deberán poder generarse en castellano, sin necesidad de conocimientos avanzados de programación.

Enriquecimiento automático de alertas

El entorno deberá disponer de capacidades de enriquecimiento automático de alertas, integrando fuentes propias de inteligencia de amenazas, repositorios OSINT, sistemas de reputación de dominios y correlaciones con incidentes anteriores. Esta funcionalidad permitirá contextualizar cada evento y mejorar la precisión de la clasificación de riesgos, reduciendo los falsos positivos y priorizando las alertas de mayor impacto operativo. Se valorará que la solución disponga de fuente de inteligencia propia, cuya calidad será determinante en la selección de la plataforma.

Detección mediante inteligencia artificial

La detección de amenazas deberá apoyarse en modelos avanzados de inteligencia artificial y aprendizaje automático, capaces de identificar comportamientos anómalos, desviaciones estadísticas o patrones de ataque no reconocidos por reglas tradicionales. Estos algoritmos deberán operar de manera continua sobre los datos históricos y en tiempo real, aprendiendo de las dinámicas del entorno sin necesidad de entrenamiento manual o etiquetado de datos.

Ejecución de playbooks automatizados



El sistema deberá garantizar la ejecución de playbooks automatizados desde la recepción de la alerta. Esta capacidad de respuesta inmediata será esencial para reducir los tiempos de detección (MTTD) y respuesta (MTTR), mejorando la capacidad de contención temprana de incidentes críticos y la resiliencia operativa de los sistemas protegidos.

4. INTEROPERABILIDAD Y REPORTING

Soporte multi-entidad y aislamiento lógico

La plataforma deberá ofrecer soporte nativo para entornos multi-tenant, posibilitando la creación de instancias lógicas independientes para cada entidad integrada en el servicio. Cada organización dispondrá de su propio espacio de trabajo, políticas de detección y paneles de control, asegurando el aislamiento de datos y la confidencialidad de la información tratada. El SOC de SOC autonómico deberá mantener una vista global consolidada que integre la información de todas las entidades, permitiendo la supervisión y gestión centralizada de incidentes.

Paneles de control personalizables

El sistema deberá incluir paneles y dashboards interactivos, personalizables según el rol del usuario, la entidad a la que pertenece y el tipo de incidente o alerta. Dichos paneles deberán actualizarse en tiempo real y ofrecer capacidades de filtrado dinámico, representación gráfica de tendencias, correlaciones temporales y métricas de rendimiento operativo.

El licitador deberá ofrecer un entorno analítico para el desarrollo de dashboards basados directamente en la misma tecnología de procesamiento que el SIEM, con integración directa y sin duplicación de datos. Además, la solución debe permitir que estos paneles se integren en una solución de Cuadros de Mando a desarrollar por el SOC de SOC, que dispondrá una serie de paneles con datos generales del Servicio prestado por el SOC de SOC. Estos paneles deben tener la capacidad de integrar datos no provenientes de eventos de seguridad, será posible integrar datos de fuentes heterogéneas, como listados de activos, formatos tabulados externos.

Interfaces de integración y APIs abiertas

La solución deberá disponer de interfaces de integración abiertas (API REST) y kits de desarrollo (SDK) que permitan la conexión con sistemas externos, tales como plataformas de ticketing, inventarios de activos, bases de datos de vulnerabilidades o servicios de threat intelligence. Estas interfaces deberán ser seguras, documentadas y compatibles con estándares industriales, asegurando la interoperabilidad del sistema dentro del ecosistema tecnológico de la Administración.

5. SEGURIDAD Y CUMPLIMIENTO

Cumplimiento del Esquema Nacional de Seguridad

La plataforma deberá cumplir plenamente con las exigencias establecidas en el Esquema Nacional de Seguridad (ENS) en su categoría Alta, garantizando la aplicación efectiva de los principios de seguridad por defecto, disponibilidad, trazabilidad y responsabilidad.



Esto implica que el sistema deberá incorporar medidas preventivas y reactivas que aseguren la protección integral de la información, el registro de toda actividad relevante y la asignación clara de responsabilidades en cada nivel de operación. Asegurando una protección adecuada frente a las amenazas que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos gestionados por la Administración. Asimismo, el adjudicatario deberá acreditar que la solución aparece en el catálogo CCN-STIC-105 en la fecha de presentación de la propuesta.

Alojamiento y tratamiento de la información en la Unión Europea

Toda la información tratada por la plataforma deberá alojarse y procesarse exclusivamente en centros de datos situados dentro del territorio de la Unión Europea, garantizando así el cumplimiento de la normativa comunitaria en materia de protección de datos personales y soberanía digital. Los centros de datos deberán contar con certificaciones de seguridad ISO/IEC 27001, así como con controles físicos y lógicos que aseguren la disponibilidad permanente y la continuidad de servicio. El proveedor deberá garantizar que no se produzca en ningún momento transferencia internacional de datos a terceros países fuera del Espacio Económico Europeo y que el servicio se adecúe plenamente a lo dispuesto por el Reglamento General de Protección de Datos (RGPD), el Reglamento (UE) 2016/679, y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

Cifrado y protección de la información

El sistema deberá implementar mecanismos de cifrado robustos y certificados que aseguren la confidencialidad y la integridad de toda la información gestionada. Los registros y datos almacenados deberán permanecer cifrados en reposo mediante el estándar AES-256, mientras que las comunicaciones y transmisiones entre los distintos componentes de la plataforma, así como entre ésta y los usuarios autorizados, deberán emplear protocolos seguros TLS 1.3 o superiores. El modelo de cifrado deberá aplicarse tanto a los datos activos como a los archivos históricos y copias de seguridad, garantizando en todo momento que las claves criptográficas estén gestionadas de forma segura y conforme a políticas verificables de control de acceso.

Retención e inmutabilidad de los registros

La plataforma deberá garantizar una retención mínima de los registros de seguridad durante un periodo no inferior a doce meses, manteniéndolos en un entorno de almacenamiento caliente que permita su consulta inmediata para investigaciones retrospectivas o auditorías de seguridad. Estos registros deberán conservarse de manera inmutable, impidiendo su modificación o eliminación por parte de los usuarios o administradores del sistema. El acceso a los registros deberá estar estrictamente controlado mediante mecanismos de autenticación fuerte, con políticas de segregación de funciones y trazabilidad completa de todas las consultas y exportaciones realizadas. Esta capacidad es fundamental para cumplir las exigencias de auditoría y responsabilidad establecidas en el ENS y las guías CCN-STIC aplicables.

Identidad federada y control de acceso

El sistema deberá ser compatible con los principales servicios de identidad federada, permitiendo la integración con mecanismos de autenticación basados en SAML 2.0 y/o



OpenID Connect (OIDC), incluyendo servicios de identidad como Active Directory Federado o equivalentes. Esta interoperabilidad permitirá aplicar políticas de autenticación centralizada, gestión de roles y control de acceso en función del perfil y responsabilidades del usuario. La plataforma deberá soportar autenticación multifactor (MFA) y auditoría completa de las sesiones, garantizando que únicamente los usuarios autorizados puedan acceder a la información o ejecutar acciones dentro del entorno operativo.

Cumplimiento del Esquema Nacional de Seguridad

La plataforma deberá cumplir plenamente con las exigencias establecidas en el Esquema Nacional de Seguridad (ENS) en su categoría Alta, garantizando la aplicación efectiva de los principios de seguridad por defecto, disponibilidad, trazabilidad y responsabilidad. Esto implica que el sistema deberá incorporar medidas preventivas y reactivas que aseguren la protección integral de la información, el registro de toda actividad relevante y la asignación clara de responsabilidades en cada nivel de operación. Asegurando una protección adecuada frente a las amenazas que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos gestionados por la Administración. Asimismo, el adjudicatario deberá acreditar que la solución aparece en el catálogo CCN-STIC-105 en la fecha de presentación de la propuesta.

Alojamiento y tratamiento de la información en la Unión Europea

Toda la información tratada por la plataforma deberá alojarse y procesarse **exclusivamente en centros de datos situados dentro del territorio de la Unión Europea**, garantizando así el cumplimiento de la normativa comunitaria en materia de protección de datos personales y soberanía digital. Los centros de datos deberán contar con **certificaciones de seguridad ISO/IEC 27001**, así como con controles físicos y lógicos que aseguren la disponibilidad permanente y la continuidad de servicio. El proveedor deberá garantizar que no se produzca en ningún momento transferencia internacional de datos a terceros países fuera del Espacio Económico Europeo y que el servicio se adecúe plenamente a lo dispuesto por el **Reglamento General de Protección de Datos (RGPD)**, el **Reglamento (UE) 2016/679**, y la **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales**.

Cifrado y protección de la información

El sistema deberá implementar mecanismos de **cifrado robustos y certificados** que aseguren la confidencialidad y la integridad de toda la información gestionada. Los registros y datos almacenados deberán permanecer **cifrados en reposo mediante el estándar AES-256**, mientras que las comunicaciones y transmisiones entre los distintos componentes de la plataforma, así como entre ésta y los usuarios autorizados, deberán emplear **protocolos seguros TLS 1.3** o superiores. El modelo de cifrado deberá aplicarse tanto a los datos activos como a los archivos históricos y copias de seguridad, garantizando en todo momento que las claves criptográficas estén gestionadas de forma segura y conforme a políticas verificables de control de acceso.



Retención e inmutabilidad de los registros

La plataforma deberá garantizar una **retención mínima de los registros de seguridad durante un periodo no inferior a doce meses**, manteniéndolos en un entorno de almacenamiento caliente que permita su consulta inmediata para investigaciones retrospectivas o auditorías de seguridad. Estos registros deberán conservarse de manera **inmutable**, impidiendo su modificación o eliminación por parte de los usuarios o administradores del sistema. El acceso a los registros deberá estar estrictamente controlado mediante mecanismos de autenticación fuerte, con políticas de segregación de funciones y trazabilidad completa de todas las consultas y exportaciones realizadas. Esta capacidad es fundamental para cumplir las exigencias de auditoría y responsabilidad establecidas en el ENS y las guías CCN-STIC aplicables.

Identidad federada y control de acceso

El sistema deberá ser **compatible con los principales servicios de identidad federada**, permitiendo la integración con mecanismos de autenticación basados en **SAML 2.0 y/o OpenID Connect (OIDC)**, incluyendo servicios de identidad como **Active Directory Federado o equivalentes**. Esta interoperabilidad permitirá aplicar políticas de autenticación centralizada, gestión de roles y control de acceso en función del perfil y responsabilidades del usuario. La plataforma deberá soportar autenticación multifactor (MFA) y auditoría completa de las sesiones, garantizando que únicamente los usuarios autorizados puedan acceder a la información o ejecutar acciones dentro del entorno operativo.

I.2. REQUISITOS NO FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

No Aplica

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Vigencia de las licencias:

Referencia	Programa	Periodo de vigencia del licenciamiento
Google Security Operations Enterprise Plus EU Subscription, o equivalente	Subscriptions/LogIngestBytes/EnterprisePlus/Europe – PrePay. Bytes of data ingested in EU for the Enterprise Plus package o equivalente	24 Meses

Los programas deben suministrarse bajo alguna modalidad de licenciamiento tal, que garantice al menos los siguientes **derechos ante el fabricante**:

Programa	Derechos durante la vigencia de las licencias
----------	---



Subscriptions/LogIngestBytes /EnterprisePlus/Europe – PrePay. Bytes of data ingested in EU for the Enterprise Plus package o equivalente.	• Derecho de uso: por acceso a la plataforma. • Derecho de actualización: parches de seguridad, versiones menores, versiones mayores. • Derecho de acceso a documentación: documentación y manuales del fabricante • Derecho de consulta al fabricante (soporte del fabricante): • Horario: 24x7 • Tiempo de respuesta: 5 días laborables
---	--

La solución ofertada debe estar homologada en el Catálogo 105 de Productos y ser STIC del CCN en, al menos, nivel alto.

La solución ofertada debe tener las guías de configuración segura y se debe incluir el enlace con la guía.

I.4. REQUISITOS DE SEGURIDAD DE LOS PROGRAMAS EN LA NUBE

Conforme al apartado III.2.3 del Pliego de Prescripciones Técnicas, las siguientes medidas¹¹ del RD 311/2022 (Esquema Nacional de Seguridad, ENS) aplican a los programas ofertados puestos a disposición en modo nube:

- [op.nub.1.2]: los programas deben ser conformes con el Esquema Nacional de Seguridad, para la categorización más alta de las enumeradas en apartado 2.4 de esta invitación.
- [op.nub.1.r1.1]: si alguno de los sistemas de información enumerados en el apartado 2.4. es de **categoría media o alta**, los programas ofertados deberán acreditar su seguridad en el momento de presentar la oferta mediante uno de los medios descritos en el apartado III.2.3 del PPT.
- [op.nub.1.r2.1]: si alguno de los sistemas de información enumerados al principio del presente apartado es de **categoría alta**, la configuración de seguridad de los programas objeto del suministro deberá realizarse según la siguiente guía CCN-STIC:
 - Guía CCN-STIC de aplicación: **la solución debe aparecer en el catálogo CCN-STIC-105 en la fecha de presentación de la propuesta.**
 - Responsable de la configuración de seguridad: La configuración debe realizarla el adjudicatario como parte de un servicio de instalación avanzada o soporte.

En todo caso, el proveedor de nube deberá disponer de un procedimiento de gestión de incidentes que dé cumplimiento a las obligaciones establecidas por el ENS y el RGPD, el cual podrá ser verificado por el organismo destinatario o por el Responsable del sistema dinámico en cualquier momento durante el periodo de vigencia de las licencias adquiridas. El procedimiento garantizará que, en caso de incidente de seguridad, el proveedor de nube entregue toda la información disponible al organismo destinatario.

¹¹ El RD 311/2022 hace referencia, en su medida [op.nub.1.1] a las guías CCN-STIC que sean de aplicación. Se trataría de la guía para el “software como servicio (SaaS)”. En el momento actual, al no estar publicada dicha guía, este requisito no es aplicable.



ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO

II.1. SERVICIOS DE INSTALACIÓN AVANZADA DE LOS PROGRAMAS A SUMINISTRAR

Alcance

El adjudicatario deberá asumir la responsabilidad integral de la puesta en marcha operativa, abarcando no solo la instalación técnica del software, sino también todas las acciones necesarias para su integración funcional, seguridad, rendimiento y operatividad dentro de la infraestructura existente. El adjudicatario deberá aportar un perfil con dedicación exclusiva y completa para coordinar y gestionar los servicios asociados al contrato.

Los servicios mínimos para ejecutar incluirán, como parte de la instalación avanzada, las siguientes actividades:

- Diseño detallado de la arquitectura de integración de la plataforma con los sistemas, plataformas y herramientas ya existentes en el organismo (EDR, firewalls, directorio activo, sistemas de identidad, herramientas de ticketing, entre otros), garantizando compatibilidad técnica, escalabilidad operativa y cumplimiento normativo (ENS, RGPD, entre otros).
- Implantación completa de la solución, incluyendo la configuración de conectores e integraciones de fuentes de log, validaciones técnicas, pruebas de ingesta de datos, pruebas de integración y pruebas funcionales, tanto en entornos de preproducción como en producción, hasta su puesta en marcha operativa.
- Personalización funcional y técnica de la solución en base a los requerimientos específicos de la Agencia, incluyendo la definición de roles, perfiles de usuario, reglas de correlación, casos de uso de detección, playbooks de respuesta, dashboards operativos, umbrales de alerta y políticas de retención y normalización de eventos.
- Configuración de la solución Cloud multi-tenant, capaz de escalar dinámicamente en función del volumen de ingesta de datos y del número de entidades incorporadas al servicio, con soporte a arquitecturas distribuidas y federadas.
- Definición e implantación de un modelo de gestión de eventos e incidentes de seguridad (SIEM/SOAR) basado en el principio de privilegio mínimo, que permita la trazabilidad completa de las alertas desde su generación hasta su cierre, incorporando flujos de trabajo automatizados y manuales conforme a los procedimientos de la Agencia.
- Uso de fuentes de inteligencia de amenazas nativa de la plataforma (*Threat Intelligence*), habilitando la correlación automática de indicadores de compromiso (IOC) con los eventos recogidos en la plataforma y la actualización continua de las reglas de detección.
- Implantación de capacidades de IA Agéntica aplicadas a la operación de la plataforma, mediante la configuración e integración de agentes autónomos de seguridad capaces de ejecutar, de forma encadenada y sin intervención humana continua, tareas de triaje de alertas, enriquecimiento de eventos con fuentes externas, investigación automatizada



de incidentes y propuesta o ejecución de acciones de respuesta. Estos agentes deberán operar bajo supervisión humana configurable, con capacidad de escalado al analista en función de umbrales de confianza predefinidos, y en estricto cumplimiento de las políticas de seguridad y privacidad del Organismo.

- Elaboración y entrega de documentación técnica y operativa completa, relativa a la instalación, configuración, integración, operación y mantenimiento de la solución, conforme a los procedimientos y estándares establecidos por la Agencia, incluyendo los procedimientos operativos de gestión de alertas, los casos de uso implantados y los flujos de actuación de los agentes de IA desplegados.
- Asignación de un Jefe de Proyecto con dedicación exclusiva del 100% por parte del adjudicatario, con experiencia demostrable en implantaciones similares, que actuará como interlocutor directo con el Responsable del Proyecto designado por la Agencia.

Aseguramiento de que todo el personal involucrado cuente con la cualificación técnica y experiencia requeridas en soluciones suministradas, incluyendo conocimiento acreditado en tecnologías de IA aplicadas a la ciberseguridad y certificaciones técnicas oficiales del fabricante.

Condiciones de ejecución

- Los trabajos deberán iniciarse a partir del día siguiente a la firma del contrato.
- Toda personalización, parametrización o adaptación de la solución, incluyendo la configuración de los agentes de IA Agéntica, deberá contar con la validación expresa del Responsable del Proyecto o del Director Técnico designado por la Agencia.
- La entrega final deberá consistir en un sistema completamente desplegado, configurado, integrado, validado y documentado, junto con la evidencia formal de la formación impartida y la transferencia de conocimiento realizada, incluyendo la operación de las capacidades de IA Agéntica habilitadas.
- La validación final de los trabajos estará sujeta a la aceptación formal por parte del Responsable del Proyecto de la Agencia, mediante acta firmada que verifique el cumplimiento de los entregables previstos.

Hitos y entregables

Hito	Descripción del hito y sus entregables	Plazo	Porcentaje de la prestación
HITO_01	<i>Ejecución completa de los servicios de instalación avanzada descritos anteriormente.</i> Entregables: • <i>Diseño de arquitectura de integración.</i> • <i>Configuración completa de la solución en todos sus módulos/licencias, incluyendo conectores de fuentes de log y reglas de correlación.</i> • <i>Integración técnica con los sistemas del organismo (EDR, firewall, IAM, directorio activo, herramientas de ticketing, etc.).</i>	<i>90 días naturales desde la entrega de licencias</i>	<i>100%</i>



	• Catálogo de casos de uso SIEM implantados y documentados. • Diseño y configuración de los agentes de IA Agéntica desplegados, con documentación de sus flujos de actuación, umbrales de confianza y mecanismos de supervisión humana. • Documentación técnica y operativa detallada. • Evidencia de realización de pruebas técnicas y funcionales. • Actas de validación funcional por parte del Jefe del Proyecto. • Plan de gestión de cambios.		
--	--	--	--

II.2. SERVICIOS DE SOPORTE DE LOS PROGRAMAS A SUMINISTRARSOPORTE TÉCNICO ESPECIALIZADO DE NIVEL 3

Alcance

El servicio deberá incluir un componente de evolución continua de las reglas de detección, correlación y automatización configuradas en la plataforma. El adjudicatario será responsable de supervisar el comportamiento de las detecciones y de incorporar mejoras basadas en el análisis de incidentes recientes, nuevas técnicas de ataque y actualizaciones publicadas por los organismos nacionales de referencia en ciberseguridad. Esta monitorización incluirá la revisión periódica de los modelos de detección, la depuración de reglas obsoletas, la optimización del rendimiento del motor de correlación y la incorporación de mecanismos de alerta temprana ante actividades anómalas. El objetivo es mantener el sistema permanentemente actualizado frente a la evolución de las amenazas y maximizar la eficacia de la detección en todo momento.

Modelos de detección basados en aprendizaje automático

El adjudicatario deberá desarrollar, mantener y ajustar modelos avanzados de detección basados en técnicas de aprendizaje automático (machine learning), tanto supervisadas como no supervisadas. Estos modelos deberán integrarse de forma nativa en la plataforma, permitiendo la identificación de comportamientos anómalos, patrones de ataque no conocidos y desviaciones estadísticas respecto a la actividad normal del entorno. El uso de machine learning permitirá evolucionar la capacidad de detección del sistema sin depender exclusivamente de reglas estáticas, incrementando la capacidad predictiva y la precisión de las alertas. El servicio incluirá la revisión periódica de los modelos, el ajuste de sus parámetros y la validación de resultados para asegurar su fiabilidad operativa.

Formación técnica avanzada

El contrato deberá contemplar un programa de formación técnica avanzada dirigido al personal del SOC autonómico, con el fin de reforzar sus competencias en materia de detección, análisis, respuesta y automatización de incidentes. Esta formación deberá impartirse por personal experto en la tecnología implantada y cubrir tanto aspectos teóricos como prácticos. Incluirá el manejo de la consola de operaciones, la interpretación de alertas, el diseño de playbooks y la aplicación de metodologías de threat hunting. El objetivo será que los analistas de la Administración adquieran una comprensión completa del entorno, sean capaces de operar con

autonomía y contribuyan a la mejora continua del servicio. La formación deberá impartirse de forma presencial o virtual, adaptada a las necesidades del personal y documentada mediante materiales oficiales.

II.2.1. DIMENSIONAMIENTO DEL SERVICIO

Los incidentes se clasificarán según su impacto en la operatividad de la solución:

- **Severidad 1 (Crítica):** Interrupción total del servicio de ingesta, correlación o visualización de eventos, o afectación directa a procesos críticos de seguridad, monitorización o análisis de amenazas.
- **Severidad 2 (Grave):** Fallos que afectan de forma relevante a funcionalidades clave de la plataforma, tales como la pérdida parcial de ingesta de fuentes prioritarias, la inoperatividad de reglas de correlación críticas, la degradación del rendimiento del sistema, limitando parcialmente la operativa sin suponer la caída total del servicio.
- **Severidad 3 (Leve):** Incidencias menores sin impacto significativo en la seguridad o funcionalidad, tales como errores en dashboards secundarios, ajustes de configuración de baja criticidad, consultas de operación habitual o reajustes de umbrales en los agentes de IA.

El Organismo trasladará al adjudicatario cuantos errores identifique en la operativa del producto.

II.2.2. ACUERDOS DE NIVEL DE SERVICIO

A efectos de cálculo del cumplimiento de los ANS, sólo computa el tiempo transcurrido dentro del horario de prestación del servicio descrito en el apartado anterior y atendiendo al dimensionamiento anterior. El adjudicatario deberá prestar los servicios de soporte y operación garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) definidos en el presente apartado, los cuales tendrán carácter obligatorio durante todo el periodo de ejecución del contrato.

1. Clasificación de incidencias

Las incidencias se clasificarán conforme a las severidades definidas en el apartado II.2.1 del presente documento:

- Severidad 1 (Crítica)
- Severidad 2 (Grave)
- Severidad 3 (Leve)

La clasificación inicial podrá ser revisada por el Responsable del Contrato cuando, a la vista del impacto real, se estime necesario.

2. Tiempos máximos de respuesta y resolución



SeveridadTiempo máximo de respuestaTiempo máximo de resolución S1

- Crítica ≤ 30 minutos ≤ 4 horas S2
- Graves ≤ 1 hora ≤ 8 horas S3
- Leves ≤ 4 horas ≤ 3 días hábiles

El tiempo de respuesta se define como el intervalo entre la notificación de la incidencia y el primer contacto efectivo del adjudicatario.

El tiempo de resolución se define como el intervalo hasta la restauración completa del servicio o la aplicación de una solución alternativa aceptada por el organismo.

3. Horario de prestación y cómputo

El cómputo de los ANS se realizará exclusivamente dentro del horario de prestación del servicio definido en el contrato. No obstante, las incidencias de Severidad 1 deberán atenderse 24x7.

4. Indicadores de seguimiento (KPIs)

El adjudicatario deberá medir, como mínimo, los siguientes indicadores:

Porcentaje de incidencias resueltas dentro del ANS comprometido

- Tiempo medio de respuesta por severidad
- Tiempo medio de resolución por severidad
- Número de incidencias recurrentes
- Disponibilidad mensual del servicio

5. Informes de nivel de servicio

El adjudicatario deberá remitir al organismo destinatario un informe mensual de ANS, que incluirá:

- Relación detallada de incidencias
- Cumplimiento de tiempos de respuesta y resolución
- Análisis de causas raíz en incidencias S1 y S2
- Medidas correctoras y preventivas adoptadas

Dichos informes formarán parte de la documentación de seguimiento del contrato a efectos de control, auditoría y PRTR.

6. Incumplimiento de los ANS

El incumplimiento de los ANS dará lugar a la aplicación de las penalidades previstas en el apartado 12 del presente documento y en el PCAP del Sistema Dinámico de Adquisición, sin perjuicio de la posible calificación del incumplimiento como grave o muy grave cuando afecte a:

- La disponibilidad del servicio
- El cumplimiento del ENS
- La continuidad del servicio de seguridad

7. Revisión y mejora continua



El organismo destinatario podrá requerir ajustes razonables en los ANS durante la ejecución del contrato, sin incremento de precio, cuando resulte necesario para garantizar la correcta prestación del servicio o adaptarse a cambios operativos debidamente justificados.

II.3. REQUISITOS DE LOS PERFILES PROFESIONALES

N/A

ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS

III.1. TRATAMIENTOS DE DATOS Y FINALIDAD DE LOS TRATAMIENTOS

Si en el apartado IV.2.1 se ha indicado que existe tratamiento de datos personales, a continuación, se señalan los datos personales que se van a transmitir y almacenar en la nube objeto del suministro:

- Categorías de interesados cuyos datos personales se tratan: No Aplica
- Categorías de datos personales tratados: No Aplica
- Datos sensibles tratados (si procede) y restricciones o garantías aplicables: No Aplica
- Naturaleza del tratamiento: No Aplica
- Finalidad(es) del tratamiento: No Aplica
- Duración del tratamiento: No Aplica

En caso de tratamiento por parte de (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento.

III.2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Serán de aplicación las medidas técnicas y organizativas para garantizar la seguridad de los datos en la nube, que resultan del análisis de riesgo o evaluación de impacto de protección de datos realizadas por el responsable del tratamiento y que se listan a continuación:

No se requieren medidas específicas.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

Contratos previos asociados con la instalación existente:

Contrato	Fecha adjudicación	Importe	Objeto
AC-015-2025 SERVICIO DE ACCESO A BASE DE DATOS ESPECIALIZADA EN ANÁLISIS AVANZADO Y MONITORIZACIÓN DE AMENAZAS PARA LAS ENTIDADES LOCALES DE LA COMUNIDAD DE MADRID	Marzo 2025	266.098,12€	Contratación de un Servicio Suscripción BBDD especializadas en análisis avanzado y monitorización de amenazas destinado a EELL de la Comunidad de Madrid

En la actualidad, la Agencia dispone de licencias del software **Google Security Operations (SecOps) SIEM Enterprise** en régimen de cesión de derecho de uso, utilizadas para dar cobertura de seguridad a diferentes Entidades Locales de menos de 20.000 habitantes (en adelante EELL<20K). Esta plataforma se ha configurado como núcleo de detección y respuesta de incidentes, integrando SIEM, SOAR y Inteligencia de Amenazas (incluida la de Mandiant), sobre un modelo de datos unificado (UDM), y se ha adaptado específicamente al entorno y a las necesidades de estas entidades.

Ante la finalización del periodo de vigencia de las citadas licencias y al tratarse de un sistema crítico para la monitorización y respuesta ante incidentes, resulta necesario disponer de las nuevas licencias de esta misma plataforma para poder continuar prestando el servicio de seguridad a dichas EELL<20K. La interrupción de licencias en un sistema como el descrito genera una **brecha de seguridad** que podría afectar a la integridad, disponibilidad y confidencialidad de los datos, dejando de funcionar servicios de detección y respuesta esenciales para cumplir con las obligaciones legales de protección de la información y con eventuales proveedores de fondos (PRTR/MRR, etc.).

El final del ciclo de vida o de la vigencia de una licencia es una **vulnerabilidad conocida en ciberseguridad**: cuando una licencia expira o deja de recibir soporte, el software deja de disponer de actualizaciones de seguridad, parches y soporte técnico, lo que incrementa su exposición a ciberataques y vulnerabilidades explotables. En este contexto, la renovación de las licencias de **Google Security Operations SIEM Enterprise** no es solo una cuestión operativa, sino una **medida esencial de ciberseguridad** para mitigar riesgos, asegurar la continuidad del



servicio y garantizar el cumplimiento de las normativas de protección de datos y de seguridad de la información aplicables.

La arquitectura actual ha sido diseñada, probada y optimizada específicamente para funcionar con las licencias y el software existente. Esto representa una inversión considerable en tiempo, dinero y recursos humanos: desarrollo de conectores, reglas de detección, playbooks de respuesta automatizada (SOAR), dashboards, integraciones con otros sistemas (SIEM, IAM, soluciones de endpoint, etc.) y formación de personal. Cambiar a un producto alternativo no equivale a una simple sustitución; implica una **migración completa** de datos, re-normalización de logs, re-diseño de reglas, re-entrenamiento del personal y, en muchos casos, reestructuración de la infraestructura para asegurar la compatibilidad. Estos costes son directos y elevados, y durante el proceso de migración existe un alto riesgo de interrupciones del servicio, pérdida de contexto analítico o fallos de seguridad no previstos, comprometiendo la disponibilidad y la integridad de los sistemas críticos.

Además, la plataforma actual **Google Security Operations SIEM Enterprise** se basa en una arquitectura cloud-native integrada, que combina SIEM, SOAR y Inteligencia de Amenazas (Mandiant, Google Threat Intelligence, VirusTotal) sobre un modelo de datos unificado. Dicha integración permite detección avanzada, correlación de eventos y respuesta automatizada, características que son difíciles de reproducir de forma equivalente en un entorno basado en múltiples herramientas distintas. Otras soluciones alternativas podrían carecer de los mismos niveles de integración, escalabilidad o madurez de correlación, lo que obligaría a reconfigurar o incluso reemplazar otros componentes de la arquitectura de seguridad.

Al mantener el producto actual, la organización se enfrenta a un conjunto de riesgos conocidos y ya gestionados, con procedimientos establecidos para la gestión de parches, monitorización de vulnerabilidades y respuesta a incidentes. La adopción de una nueva plataforma, por muy avanzada que sea, implica un nuevo conjunto de riesgos desconocidos y un periodo de adaptación que deteriora temporalmente la capacidad de detección y respuesta, justo en un contexto en el que la estabilidad del SOC/CSIRT es estratégica para la ejecución de programas financiados por fondos MRR y PRTR.

En consecuencia, la **justificación de la contratación directa**, mediante el Acuerdo Marco SDA-25, del siguiente nivel de producto **Google Security Operations SIEM Enterprise**, se basa en la necesidad de mantener la continuidad operativa y la estabilidad de la arquitectura de seguridad, en la mitigación de riesgos derivados de la interrupción de licencias o de la migración a una nueva plataforma, y en la optimización económica al evitar la invalidación de la inversión ya realizada en integración, configuración y formación. La renovación de las licencias actuales representa, desde un punto de vista técnico, de seguridad y de coste, la opción más segura, estable y viable para garantizar la protección de la información y la prestación continuada del servicio de seguridad a las EELL<20K, sin comprometer la madurez alcanzada en la estrategia de detección y respuesta de incidentes.



ANEXO V MODELO DE DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS

Organismo destinatario:	
AM/SDA:	SDA 25/2022 LOTE 4
Propuesta de adjudicación/Expediente organismo destinatario	
Objeto:	

D./D^a:....., con D.N.I. nº:....., actuando en nombre propio / en representación de (a empresa licitadora) con N.I.F.:....., con domicilio (de la empresa licitadora) en (calle/plaza/etc.):....., nº:....., Población:....., Provincia:....., y código postal:.....

En relación con el expediente de contratación arriba referenciado y de conformidad con lo dispuesto en los pliegos reguladores del SDA y en el documento de invitación objeto de la licitación.

DECLARA

☐ Que dispone de información del proveedor de los productos en nube incluidos en la oferta presentada, la cual permite asegurar que dicho proveedor (**INDICAR DENOMINACIÓN DEL PROVEEDOR DE NUBE**) en su condición de encargado y los programas ofertados cumplen, en lo que les es directamente aplicable, las obligaciones que establecen el Reglamento General de Protección de Datos (RGPD), la normativa española de protección de datos y otra normativa jurídica que resulte de aplicación. En concreto, que los datos están ubicados y los tratamientos se realizan en las regiones descritas en el apartado 9.4 del documento de invitación, sin más excepciones que las transferencias internacionales que se listan a continuación:

Denominación del producto ofertado y del proveedor de nube	
Documentación vinculante del proveedor de nube aplicable	
Establecimiento del proveedor de nube	
Detalle de las transferencias internacionales previstas	



Detalle de los subencargados y su ubicación	
Detalle de las medidas de seguridad aplicables	

☐ Que la documentación vinculante del proveedor de nube antes referida constituye un acto jurídico previsto en el artículo 28.3 del RGPD, que vincula al proveedor de nube respecto del responsable del tratamiento del organismo destinatario durante toda la vigencia de las licencias. Para ello, se compromete a aportar al responsable del tratamiento la mencionada documentación vinculante, con carácter previo a la ejecución del contrato (el suministro de las licencias), y a no iniciar dicha ejecución si no es de conformidad con el responsable.

Y para que así conste y surta los efectos oportunos, expido y firmo la presente declaración,

(Fecha, firma y nombre completo del representante legal)

Fdo. electrónicamente



ANEXO VI MANIFESTACIÓN DE CONFORMIDAD DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS DEL ORGANISMO DESTINATARIO

Organismo destinatario:	
AM/SDA:	SDA 25/2022 LOTE 4
Propuesta de adjudicación/Expediente organismo destinatario	
Objeto:	

Vista la declaración responsable de cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos (RPGD)) emitida por el apoderado actuando en representación de la empresa **INCLUIR NOMBRE DE EMPRESA** con NIF **RELLENAR**, licitador del procedimiento de contratación de referencia.

MANIFIESTO

Que puede considerarse que el proveedor de nube ofrece garantías suficientes para efectuar el tratamiento de datos de carácter personal.

Indicar nombre y cargo. Firma electrónica.



ANEXO VII ENTREGAS PARCIALES

No Aplica

ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO

La garantía extendida que debe prestar el adjudicatario durante todo el periodo de vigencia de las licencias se rige por lo descrito en el apartado III.8 del Pliego de Prescripciones Técnicas:

- Soporte de nivel 1 y nivel 2 prestado por el adjudicatario a petición del organismo destinatario, en los términos descritos en el PPT;
- Soporte del adjudicatario al organismo para el acceso a la garantía del fabricante (acceso al soporte de nivel 3), en los términos descritos en el PPT;
- Soporte a la instalación de actualizaciones, en los términos descritos en el PPT;
- Cobertura ante posibles problemas jurídicos derivados de la aplicación de las cláusulas de *términos y condiciones* del fabricante, en los términos descritos en el PPT.

Horario de contacto: Haga clic o pulse aquí para escribir texto.

Acuerdos de nivel de servicio:

Horario de contacto: 24x7 Acuerdos de nivel de servicio: El proveedor debe ofrecer una arquitectura resiliente capaz de ofrecer SLA de al menos 99.99% en disponibilidad del servicio y latencia media garantizada de 100 ms para el 95th del percentil del tráfico mensual, incorporando las funcionalidades de seguridad activas junto con inspección DLP y threat scanning.

Estos valores deben contemplar siempre que se realizan con inspección de tráfico HTTPS, Threat scanning, DLP, con un 99.999% de uptime y con 100% Captura de virus conocidos. Estos valores deben indicarse por transacción.

No se admitirán exclusiones en los acuerdos de nivel de servicio SLA como, por ejemplo:

- Excluir el tiempo necesario para analizar un contenido desde un punto de vista de ciber amenazas (Threat scanning) y control de fuga de información (DLP).
- Excluir upgrades no planeados
- Excluir de los resultados request o respuestas más grande de 1MB.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

ANEXO IX 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 EL SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (SDA 25/2021; Expediente 2022/48), 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.¹²
- **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

¹² 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 incurso en supuesto alguno a los que se refiere el artículo 71 de la LCSP.”



ANEXO X DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

Don/Dña, 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 037¹³ 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 invitación 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:

(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:

¹³ 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.





La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **0981731572917942371068**

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 específicos financiados¹⁴ 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.

¹⁴ O es susceptible de ser financiado en caso de no haberse aún confirmado la selección por las autoridades correspondientes.



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.

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 15. Inversión 07**

C15.I07.P06.S61.SI01.PROVISIONAL.03 – Actuación L4-Programa de refuerzo de la estrategia regional de ciberseguridad

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:

a) Obligaciones del componente/inversión por el **etiquetado verde**:

No existen obligaciones específicas

b) 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 el suministro de licencias software destinadas a componer la arquitectura de ciberseguridad. Esta actuación se enmarca dentro del 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, centrada exclusivamente en la adquisición de soluciones digitales, permite justificar una contribución del 100% al etiquetado digital, conforme a los criterios establecidos por la Comisión Europea y la normativa nacional aplicable. En particular:

- Las licencias a suministrar están directamente relacionadas con la digitalización de servicios y procesos.
- Se trata de una actuación que, por sí misma, constituye una inversión digital.

No se incluyen elementos físicos o no digitales que requieran ponderación o exclusión

- c) 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. Las prestaciones de suministro de licencias de software, en general, no están

directamente afectadas por los seis objetivos medioambientales definidos en el Reglamento (UE) 2020/852, ya que:

- No implican emisiones significativas de gases de efecto invernadero.
- No generan residuos físicos ni impacto directo sobre recursos hídricos, biodiversidad o ecosistemas.
- No requieren infraestructuras físicas que puedan alterar el entorno natural.

Sin embargo, sí deben cumplir con el principio DNSH (*Do No Significant Harm*), lo que implica que deben demostrar que no causan un perjuicio significativo a ninguno de los seis objetivos medioambientales durante todo el ciclo de vida del proyecto.

Obligaciones específicas para licencias software:

- Evaluación del ciclo de vida
 - Aunque el software no tiene impacto físico directo, se debe considerar el uso de recursos asociados (por ejemplo, servidores, energía para funcionamiento, etc.).
 - Si el software se instala en centros de datos, estos deben cumplir con criterios de eficiencia energética y sostenibilidad.
- Declaración responsable DNSH
 - Se debe incluir una declaración responsable en el expediente, indicando que la actividad no causa perjuicio significativo a los seis objetivos medioambientales
 - Esta declaración debe considerar aspectos indirectos como el consumo energético del software, su contribución a la economía circular (por ejemplo, si permite reducir papel o procesos físicos), etc.
- Clasificación como actividad de bajo impacto
 - El suministro de licencias suele clasificarse como actividad de bajo impacto ambiental, lo que simplifica la evaluación DNSH. Aun así, se recomienda



completar el cuestionario de autoevaluación DNSH disponible en las guías del PRTR

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

Sin perjuicio de las causas de modificación previstas en el documento de invitación, 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 ESPECÍFICOS FINANCIADOS EN EL PRTR

(Marcar si procede y definir, en su caso, cuantías)

En caso de incumplimiento o cumplimiento defectuoso por el contratista de los compromisos adquiridos en base a las obligaciones establecidas en este documento de invitación 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:

() 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. *(Definir cuantía o % si se marca la penalidad)*

() Por incumplimiento. *(Definir % si se marca la penalidad)*

() Por incumplimiento de las obligaciones asociadas al DNSH del componente/inversión: *(Definir % si se marca la penalidad)*

() Otras penalidades
(Definir)

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 específicos financiados con cargo al Plan de Recuperación, Transformación y Resiliencia (PRTR).

