

**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 LICENCIAS DE ACCESO A UNA PLATAFORMA
SOFTWARE DE CIBERSEGURIDAD PARA LA DETECCIÓN,
ANÁLISIS Y GESTIÓN DEL RIESGO DE CIBERSEGURIDAD
ASOCIADO A LOS CANALES DE COMUNICACIÓN DE LA
COMUNIDAD DE MADRID, EN EL MARCO DEL PRTR,
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.

TÉRMINOS Y CONDICIONES



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**

1.	ORGANISMO DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO .	4
2.	LOTE, TITULO Y OBJETO DEL CONTRATO ESPECÍFICO.....	4
2.1.	Lote, título y objeto	4
2.2.	Características principales de las prestaciones.....	5
2.3.	Tratamiento de datos de carácter personal por parte del adjudicatario	6
2.4.	Categorización conforme al Esquema Nacional de Seguridad (ENS)	6
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.....	10
4.6.	Contrato financiado con cargo al presupuesto de la Unión Europea	11
5.	LUGAR Y CONDICIONES DE LA ENTREGA.....	11
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN	12
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	12
7.1.	Ponderación de los criterios de adjudicación	12
7.2.	Fórmula aplicable al criterio precio	13
7.3.	Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio	13
7.3.1.	Criterios evaluables automáticamente mediante fórmulas	13
7.3.2.	Fórmulas para la evaluación automática de los criterios	13
7.4.	Criterios cuya cuantificación depende de un juicio de valor	14
7.4.1.	Criterios y ponderación.....	14
7.4.2.	Método de valoración y documentación.....	14
8.	OFERTAS ANORMALMENTE BAJAS.....	14
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA.....	15
9.1.	Obligaciones generales.....	15
9.2.	Otras condiciones de ejecución del contrato.....	16
9.3.	Obligaciones de seguridad en cumplimiento del ens	16
9.4.	Obligaciones relativas al cumplimiento de las condiciones de los programas ofertados en modalidad de nube cuando exista tratamiento de datos personales	16
10.	PAGO Y FACTURACIÓN	17
10.1.	Pago del precio	17
10.2.	Condiciones de presentación de las facturas.....	17
11.	GARANTÍA DE LOS BIENES	18



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: 1018620018705260308196

12.	PENALIDADES	19
12.1.	Penalidades fijadas en el sistema dinámico de adquisición.....	19
12.2.	Fórmula para la aplicación de penalidades.....	20
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO	20
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS.....	20
	ANEXO I PRESCRIPCIONES TÉCNICAS.....	23
I.1.	Requisitos funcionales de los programas a suministrar.....	23
I.2.	Requisitos no funcionales de los programas a suministrar.....	31
I.3.	Periodo de vigencia y modalidad de licenciamiento.....	31
I.4.	Requisitos de seguridad de los programas en la nube.....	32
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO	33
II.1.	Servicios de instalación avanzada de los programas a suministrar.....	33
II.2.	Servicios de soporte de los programas a suministrar	33
II.2.1.	Dimensionamiento del servicio	33
II.2.2.	Acuerdos de nivel de servicio	33
II.3.	Requisitos de los perfiles profesionales.....	33
	ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS	34
III.1.	Tratamientos de datos y finalidad de los tratamientos	34
III.2.	Medidas técnicas y organizativas.....	34
	ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE.....	35
	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	36
	ANEXO VI Manifestación de conformidad del responsable del tratamiento DE LOS DATOS DEL ORGANISMO DESTINATARIO	39
	ANEXO VII ENTREGAS PARCIALES	40
	ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO	40
	ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN.....	41
	ANEXO X DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA	42
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	43
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea 44	
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR	46



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: 1018620018705260308196

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 licencias de acceso a una plataforma software de ciberseguridad para la detección, análisis y gestión del riesgo de ciberseguridad asociado a los canales de comunicación de la Comunidad de Madrid, en el marco del PRTR, financiado por la unión europea – NEXTGENERATIONEU

Objeto del contrato:

El presente pliego tiene por objeto el **suministro de licencias de acceso a una plataforma de software de ciberseguridad en modalidad SaaS (Software as a Service)**, orientada a la detección, análisis y gestión continua del riesgo humano asociado a los canales de comunicación utilizados por la Comunidad de Madrid, por un período de **36 meses**.

Las capacidades funcionales de la solución se ofrecen de forma integral como prestaciones inherentes al propio suministro de licencias. Con carácter accesorio, y a efecto de garantizar la correcta entrega y operatividad de las mismas, el contrato incluirá la activación y puesta a disposición de las licencias en el entorno de la organización, así como el soporte para el correcto funcionamiento durante la vigencia del contrato por parte del fabricante.

El riesgo que emerge en los canales de comunicación motivado por la interacción humana constituye hoy el principal vector de exposición en ciberseguridad. Los informes de referencia del sector —Verizon

Data Breach Investigations Report, ENISA Threat Landscape, IBM X-Force— coinciden en que más del 80% de las brechas de seguridad tienen un componente de comportamiento humano como factor habilitante. Sin embargo, la mayoría de las organizaciones carecen de instrumentos de medición objetiva que permitan cuantificar, monitorizar y reducir este riesgo de forma sistemática y basada en evidencia.

La plataforma objeto de esta contratación deberá cubrir, como mínimo, las siguientes capacidades funcionales, en el marco del PRTR cofinanciado por la Unión Europea – NextGenerationEU, 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.

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**:

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].



☒ 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 **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: 15 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.

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.



☐ 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: 180 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.
 - ☐ 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 (€)
1.508.928,42 €	316.874,97 €	1.825.803,39 €

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)	1.508.928,42 €	316.874,97 €	1.825.803,39 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario			
Servicio de soporte, a prestar por el adjudicatario			
TOTAL	1.508.928,42 €	316.874,97 €	1.825.803,39 €

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	TOTAL
El presente pliego tiene por objeto el suministro de licencias de acceso a una plataforma software de ciberseguridad para la detección, análisis y gestión del riesgo de ciberseguridad asociado a los canales de comunicación utilizados por los empleados de la Comunidad de Madrid.	1.825.803,39€	1.825.803,39€

La licitación se financia con fondos MRR RETECH.

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	
Resto costes directos	1.347.257,52 €
Costes indirectos + Gastos generales + Beneficio industrial	161.670,90 €
Total sin IVA	1.508.928,42 €

Justificación:

El objeto del contrato es la adquisición de licencias de software. Esto implica que los costes directos abarcan la totalidad de los gastos asociados a la adquisición de la licencia incluyendo el soporte técnico del fabricante y el derecho a actualizaciones durante la vigencia del contrato.

El presente contrato tiene naturaleza de suministro de licencias software en modalidad SaaS, no incluyendo servicios profesionales, de implantación, operación o soporte prestados por el adjudicatario.

El soporte técnico, mantenimiento correctivo y evolutivo, actualizaciones de seguridad y mejoras funcionales se encuentran incluidos como derechos inherentes al licenciamiento del fabricante y no constituyen prestaciones de servicios diferenciadas.

Asimismo, para la determinación del precio detallado en la tabla anterior, se han considerado un 6% en concepto de gastos generales y un 6% en concepto de beneficio industrial.

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.

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:

Haga clic o pulse aquí para escribir texto.

- Circunstancias admitidas para modificar el contrato específico⁵:
 - No aplica

⁵ Entre las circunstancias que se pueden señalar deben precisarse las admitidas en el apartado 27.17 del PCAP del SDA 25/2022.



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 OCHO MIL NOVECIENTOS VEINTIOCHO EUROS CON CUARENTA Y DOS CÉNTIMOS**. euros, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	1.508.928,42 €
Importe máximo por modificación prevista, sin IVA	Haga clic o pulse aquí para escribir texto.
TOTAL	1.508.928,42 €

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

Código de operación/Proyecto/Iniciativa: C15.I07.P06.S61.SI01.PROVISIONAL.03

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 PONDERACIÓN⁶

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

⁶ Criterios de valoración conforme a las previsiones del apartado 27.5.4 del PCAP.

N/A	N/A	N/A
-----	-----	-----

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:

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

NO APLICA

7.3.2. FÓRMULAS PARA LA EVALUACIÓN AUTOMÁTICA DE LOS CRITERIOS

Función **Maximizar**:

$$C_i = P * \frac{X_i}{X_{máx}}$$

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;
- $X_{máx}$ 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

No se han establecido criterios que dependan de un juicio de valor.

7.4.1. CRITERIOS Y PONDERACIÓN

No Aplica

7.4.2. MÉTODO DE VALORACIÓN Y DOCUMENTACIÓN

No Aplica

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: *indicar % o importe*.

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

No se establecen otras condiciones.

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 RGPD⁷.

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.

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.

⁷ 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>.



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

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

- Órgano de contratación: Dirección General de Racionalización y Centralización de la Contratación - E04962703.
- Órgano responsable del contrato específico (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-021-2026.

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 Grave: 5% Muy grave: 10%		Valor fijado en el SDA
Incumplimiento de las obligaciones de información y pago sobre suministradores y subcontratistas.	2% del importe del subcontrato Grave: 5% Muy grave: 10%		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

Las ofertas se presentarán obligatoriamente en formato electrónico, a través de la PLACSP⁸ u otra plataforma de contratación a disposición del organismo.

Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa⁹.

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

La oferta económica **deberá incluir como mínimo 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, en la siguiente dirección:

⁸ Plataforma de Contratación del Sector Público: <https://contrataciondelestado.es/wps/portal/quiasAyuda>

⁹ 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.



https://contratacioncentralizada.gob.es/documents/32143/48667/Modelos+de+Oferta+SDA25_2022.zip/b255fa33-a721-b657-d308-743f00fb56b4?t=1759159939180

La omisión de este desglose será causa de exclusión de la oferta.

Además, la oferta deberá incluir el **desglose detallado** de los precios individuales de cada producto o servicio incluido. Junto con la invitación, el organismo destinatario podrá adjuntar un modelo de oferta económica más detallado, que complemente la información exigida en el citado modelo de oferta.

La oferta técnica deberá contener la siguiente documentación:

- Relación de los programas en la modalidad de licenciamiento que se ofertan
- Matriz de cumplimiento justificativa de los requisitos de la plataforma ofertada
- La información de los requisitos mínimos de los productos o referencias a las fichas técnicas o catálogos que permitan acreditar los criterios automáticos:
 - *No aplica al no establecerse criterios automáticos*
- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - *No aplica al no establecerse criterios automáticos*
- Si la oferta incluye programas que forman parte de la arquitectura de seguridad del organismo **se deberá incluir la acreditación de los requisitos de seguridad** exigidos por cualquiera de los medios descritos en el apartado III.2.2 o III.2.3 del PPT, según corresponda. La falta de acreditación será motivo de exclusión de la oferta.

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.

- *El organismo detallará si en este apartado debe incluirse de forma necesaria algún documento para valorar los criterios sujetos a juicio de valor*

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://contratacioncentralizada.gob.es/documents/32143/48667/02-Modelo-DI-SDA-25-2022-junio-2025.docx/08339f7e-2487-e470-3625-f4c1d2d0e5d3>



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, PREVALECEERÁN ESTOS ÚLTIMOS.

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

EL TITULAR DEL ÓRGANO DESTINATARIO (CARGO): El Consejero Delegado de la agencia de Ciberseguridad de la Comunidad de Madrid.

Firmado electrónicamente (nombre y apellidos): **D. 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: **1018620018705260308196**

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

Los requisitos funcionales recogidos en el presente apartado definen las capacidades mínimas que deberá proporcionar la plataforma a suministrar, en modalidad SaaS, para la detección, análisis y gestión del riesgo de ciberseguridad asociado a los canales de comunicación utilizados por los empleados, así como para la generación de alertas e informes y la integración mediante API con los sistemas corporativos. Las prescripciones se formulan en términos de prestaciones y resultados esperados.

A efectos del suministro, el licitador deberá identificar en la siguiente tabla el/los programas ofertados y el modelo de licenciamiento asociado:

Part Number	Programa	Cantidad
ZP-COR-001 o equivalente	Zepo Platform SaaS - Acceso a la plataforma Zepo en modalidad SaaS (cloud AWS EU). Incluye consola de administración, dashboards en tiempo real y gestión multitenant o solución equivalente.	Hasta 150.000

La plataforma suministrada deberá cumplir, como mínimo, con los siguientes requisitos:

Requisito de producto por compatibilidad. De conformidad con lo indicado en el **Anexo IV** (necesidad de productos concretos por compatibilidad con instalación existente), el suministro objeto del presente contrato deberá corresponder a la plataforma **ZEPO**, o, en su caso, a una solución **equivalente únicamente en la medida en que garantice la compatibilidad técnica** con la instalación existente y la **continuidad metodológica y comparabilidad** de las métricas e indicadores ya implantados, sin discontinuidades en la serie histórica.

REQUISITOS GENERALES (PLATAFORMA ZEPO O EQUIVALENTE CONFORME A ANEXO IV)

REQ 0. Requisito transversal de compatibilidad con ZEPO y continuidad de métricas.

La solución ofertada deberá ser **ZEPO** o equivalente (únicamente en los términos estrictos de compatibilidad del **Anexo IV**) y deberá garantizar, como mínimo: (i) **continuidad operativa** sin necesidad de reimplantación completa; (ii) **reutilización** de la configuración existente, modelos de medición, indicadores, cuadros de mando e integraciones; (iii) **preservación de la serie histórica** de métricas ya recopiladas y su comparabilidad; y (iv) **interoperabilidad** con los conectores/API ya disponibles en la instalación existente. El licitador deberá describir de forma explícita cómo se asegura esta compatibilidad y continuidad.

REQ 1. Evaluación y cuantificación del riesgo conductual.

Medición objetiva, continua y automatizada del nivel de riesgo de ciberseguridad asociado al comportamiento de cada identidad digital, cada unidad operativa y de la organización en su conjunto.



La cuantificación deberá basarse en datos empíricos de comportamiento observado, no en autoevaluaciones ni cuestionarios declarativos.

A efectos de este Anexo, los requisitos se entenderán referidos a la plataforma **ZEPO** (o equivalente en los términos estrictos de compatibilidad establecidos en el **Anexo IV**).

REQ 2. Detección de amenazas de ingeniería social.

Análisis automatizado de comunicaciones y artefactos digitales a través de múltiples canales para identificar intentos de suplantación, fraude, manipulación o exfiltración, generar un veredicto trazable y activar acciones proporcionales. Estas capacidades deberán proporcionarse en la plataforma **ZEPO** o equivalente (en los términos estrictos de compatibilidad del **Anexo IV**).

REQ 3. Analítica conductual avanzada y generación de informes.

Producción automática de informes analíticos, dashboards operacionales y reportes ejecutivos que transformen los datos de comportamiento en inteligencia accionable para la toma de decisiones en materia de riesgo. La plataforma deberá ir más allá de las métricas simples (tasa de clic) para ofrecer un análisis multidimensional del comportamiento que identifique las causas raíz del riesgo, no solo sus síntomas. Estas capacidades deberán proporcionarse en la plataforma **ZEPO** (o equivalente en los términos estrictos de compatibilidad del **Anexo IV**).

REQUISITOS DEL MODELO ANALÍTICO DE RIESGO CONDUCTUAL

Los requisitos del presente bloque aplican a la plataforma **ZEPO** o equivalente (en los términos estrictos de compatibilidad del **Anexo IV**) y deberán acreditarse manteniendo la continuidad metodológica y la comparabilidad de métricas.

REQ 4.1 Índice de riesgo conductual (Risk Score)

La plataforma implementará un modelo cuantitativo de evaluación del riesgo conductual que asigne a cada identidad, unidad operativa y a la organización en su conjunto un índice de riesgo conductual numérico, comparable y trazable en el tiempo. Este índice será el indicador central del sistema y deberá cumplir las siguientes características:

Multidimensionalidad. El índice no se limitará a una única métrica (como la tasa de clic en phishing), sino que integrará múltiples dimensiones del comportamiento de seguridad. Como referencia conceptual, se espera un enfoque similar al de las ontologías conductuales de seguridad que mapean comportamientos observables contra resultados de riesgo verificables. El modelo deberá considerar, como mínimo, las siguientes dimensiones:

- **Exposición a amenazas de ingeniería social:** medida a partir del volumen, severidad, recurrencia y distribución de señales sospechosas o maliciosas detectadas a través de los distintos canales integrados, considerando no sólo la existencia de la señal sino también su criticidad y profundidad potencial de compromiso.
- **Capacidad de detección y reporte:** medida a través de la tasa de reporte de amenazas simuladas y reales, el tiempo de reacción y la calidad del reporte (categorización, descripción, nivel de alerta).
- **Consistencia del patrón de exposición:** evaluación de la estabilidad del riesgo en el tiempo, distinguiendo entre concentraciones puntuales y patrones persistentes por identidad, unidad o canal.



- **Perfil de exposición:** ponderación del riesgo en función del rol organizativo, el nivel de acceso a sistemas críticos, la responsabilidad sobre información sensible y la visibilidad externa de la identidad.

Granularidad a tres niveles. El índice se calculará y presentará en tres niveles de agregación: identidad individual (para identificar usuarios de alto riesgo), unidad operativa o departamento (para comparar el rendimiento relativo de las distintas áreas) y organización completa (para seguimiento ejecutivo y benchmarking).

Actualización continua. El índice se recalculará de forma automática y continua a medida que se recopilen nuevos datos de comportamiento, sin necesidad de intervención manual. Cada simulación ejecutada, cada amenaza reportada y cada interacción con la plataforma alimentarán el modelo de riesgo en tiempo real.

Fundamentación en datos observados. El modelo analítico deberá estar sustentado en señales empíricas, telemetría verificable y criterios trazables, no en valoraciones subjetivas ni en clasificaciones opacas imposibles de auditar.

REQ 4.2. Perfilado automático de identidades

La plataforma realizará un perfilado automático y continuo de cada identidad a partir de fuentes de datos complementarias:

Atributos organizativos. Importados desde los directorios corporativos (Active Directory, Azure AD, Google Workspace), incluyendo: rol y posición jerárquica, departamento y unidad operativa, nivel de acceso a sistemas y aplicaciones críticas, responsabilidad sobre datos sensibles o clasificados, ubicación geográfica e idioma, y antigüedad en la organización.

Datos observados de comunicación. Recopilados directamente por la plataforma a partir del análisis de los canales integrados, incluyendo: historial de señales detectadas, patrones de reporte de amenazas reales, evolución temporal del índice de riesgo, frecuencia de exposición por canal y respuesta diferenciada según el tipo de técnica de ingeniería social empleada (urgencia, autoridad, reciprocidad, escasez o familiaridad).

Enriquecimiento con telemetría externa. El perfil de riesgo de cada identidad se podrá enriquecer mediante la integración con fuentes externas de datos de seguridad: plataformas SIEM para correlacionar eventos de seguridad con comportamiento en simulaciones, herramientas de gestión de identidades para incorporar datos de acceso y privilegios, y sistemas GRC para contextualizar el riesgo dentro del marco de gobernanza de la organización. Esta correlación entre datos internos y externos permitirá construir un perfil de riesgo integral que trascienda los límites de la propia plataforma.

REQ 4.3 Modelo de madurez organizacional

Se valorará que la plataforma incorpore un modelo de madurez en gestión de riesgo conductual que permita evaluar y hacer seguimiento de la posición de la organización en un marco de referencia estructurado. El modelo contemplará, como mínimo, las siguientes dimensiones: nivel de visibilidad del riesgo conductual, cobertura de la evaluación (porcentaje de identidades evaluadas activamente), sofisticación de los mecanismos de medición, efectividad de las intervenciones de reducción del riesgo y grado de integración con los procesos de gobernanza de seguridad de la organización.



REQUISITOS DE IDENTIFICACIÓN DE FACTORES Y COMPORTAMIENTOS DE RIESGO

REQ 5. Identificación de factores y comportamientos de riesgo

La calidad, cobertura y fiabilidad del análisis determinan directamente la efectividad del sistema. La plataforma deberá incorporar un motor de detección multicanal que cubra los vectores de comunicación que se describen a continuación.

La plataforma analizará de forma específica enlaces, redirecciones, dominios, adjuntos y otros artefactos compartidos a través de los canales integrados. Las páginas de destino asociadas serán inspeccionadas cuando resulte técnicamente viable, incluyendo expansión de redirecciones, verificación de reputación, detección de dominios homógrafos o tipográficamente similares, y análisis de objetos embebidos o contenedores comprimidos.

Cada interacción observada quedará registrada con el mayor nivel de detalle disponible, incluyendo canal de origen, identidad implicada, artefacto analizado, hallazgos, acción ejecutada y referencias cruzadas con otras señales relacionadas.

Se valorará que la plataforma incorpore capacidad de analizar señales procedentes de canales de voz y videollamada, incluyendo metadatos de llamadas, invitaciones, transcripciones, archivos intercambiados o indicadores contextuales de suplantación cuando estos estén disponibles a través de integraciones nativas o de mecanismos oficialmente soportados por la plataforma del cliente.

La compatibilidad mínima exigida será con Microsoft Teams, Google Meet y Zoom, al menos en los componentes de integración y enriquecimiento que las APIs permitan. Se valorará especialmente la capacidad de identificar solicitudes urgentes, instrucciones sensibles y patrones anómalos en conversaciones que tradicionalmente se perciben como seguras y de alta confianza.

La plataforma dispondrá de capacidades de análisis para comunicaciones cursadas a través de plataformas de colaboración y mensajería corporativa, incluyendo Microsoft Teams, Slack y otras herramientas equivalentes que la organización utilice. El análisis deberá cubrir mensajes, enlaces, archivos compartidos, invitaciones, conversaciones directas y elementos contextuales disponibles a través de las APIs oficialmente soportadas.

La medición del riesgo será granular: recepción de la señal, clasificación inicial, hallazgos asociados, acción ejecutada, tiempo de respuesta y, cuando la telemetría esté disponible, interacciones relevantes del usuario con el contenido analizado. El sistema correlacionará automáticamente el comportamiento observado en mensajería corporativa con el comportamiento observado en otros canales para enriquecer el perfil de riesgo multicanal.

La arquitectura deberá ser agnóstica de canal. La incorporación de nuevos canales de comunicación relevantes durante la vigencia del contrato —por ejemplo, mensajería adicional, entornos de colaboración o futuros conectores oficialmente soportados— requerirá únicamente el desarrollo o activación del conector correspondiente, sin necesidad de rediseñar los motores de análisis, veredicto, trazabilidad y reporting.

Adicionalmente, se requerirán capacidades transversales en el motor de detección. En particular:

Correlación multicanal. La plataforma permitirá la correlación de señales que combinen múltiples canales de forma secuencial o simultánea —por ejemplo, un mensaje en Teams o Slack y una



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**

posterior llamada de verificación— con el fin de identificar campañas coordinadas y patrones de ataque híbridos.

Mecanismo de reporte integrado. La plataforma proporcionará, cuando el canal lo permita, mecanismos nativos para reportar comunicaciones sospechosas con un único clic o una acción equivalente. El complemento o flujo de reporte será personalizable en identidad visual, categorización y destino operativo, y dispondrá de integración con herramientas como Microsoft Defender for Office 365, SIEM o sistemas de ticketing para el tratamiento automatizado de las comunicaciones reportadas.

Trazabilidad y explicabilidad. Cada señal quedará registrada con un historial completo de recepción, módulos ejecutados, hallazgos generados, puntuación asignada, acción tomada y resultado final. El analista deberá poder reconstruir el razonamiento del sistema sin necesidad de soporte del proveedor.

REQUISITOS DE EMULACIÓN DE COMUNICACIONES FRAUDULENTAS MULTIVECTOR

REQ 6. Emulación de comunicaciones fraudulentas multivector

La plataforma deberá permitir la emulación controlada, automatizada y a escala de comunicaciones fraudulentas a través de múltiples vectores y canales de interacción utilizados habitualmente en el entorno corporativo, incluyendo, entre otros, mensajería instantánea, SMS, llamadas de voz, videoconferencias y cualquier otro canal digital que resulte relevante para la organización.

Estas capacidades deberán estar orientadas a reproducir de forma realista las técnicas de ingeniería social y fraude utilizadas en escenarios reales de amenaza, con el objetivo de identificar patrones de comportamiento, detectar vulnerabilidades en la interacción con distintos canales y generar información accionable sobre el nivel de riesgo de la organización.

Los resultados obtenidos a partir de estas emulaciones deberán integrarse en indicadores, métricas y análisis que permitan una comprensión profunda, continua y contextualizada de la postura de ciberseguridad de la organización, facilitando la priorización de acciones de mitigación, y fortalecimiento de controles.

REQUISITOS DE INDICADORES CLAVE DE RENDIMIENTO (KPIs)

REQ 7. Indicadores clave de rendimiento (KPIs)

La plataforma deberá calcular, presentar y permitir la exportación de, como mínimo, los siguientes indicadores clave de rendimiento. Los KPIs se organizan en cuatro categorías analíticas.

REQ 7.1 KPIs de susceptibilidad y exposición al riesgo

- **Tasa de señales sospechosas o maliciosas por vector de comunicación.** Porcentaje y volumen absoluto de señales clasificadas como Suspicious o Malicious, desglosadas por cada canal integrado. Esta métrica permite identificar en qué canales la organización presenta mayor exposición.
- **Tasa de compromiso profundo observable.** Porcentaje de identidades que, cuando la telemetría del canal lo permite, llegan a la acción de máximo riesgo asociada a una señal real: apertura de



enlace, descarga de adjunto, revelación de información o validación de una solicitud sensible. Distingue el riesgo superficial del riesgo crítico.

- **Índice de riesgo medio.** Valor medio del índice de riesgo a nivel de organización, unidad operativa e identidad, con segmentación por cualquier atributo del directorio.
- **Distribución del riesgo.** Distribución estadística de las identidades por tramos de riesgo (bajo, medio, alto, crítico). Permite visualizar la proporción de la organización que se encuentra en cada zona de riesgo y la evolución de dicha distribución en el tiempo.
- **Identities de riesgo persistente.** Número y porcentaje de identidades que permanecen en tramo de riesgo alto o crítico durante más de un periodo consecutivo.
- **Tasa de reincidencia.** Porcentaje de identidades que vuelven a incurrir en interacciones de riesgo o que reciben de forma recurrente señales de naturaleza equivalente sin que el índice de riesgo se reduzca de forma material.
- **Exposición por técnica de persuasión.** Desglose del riesgo según la técnica de ingeniería social detectada en la comunicación: urgencia, autoridad, escasez, reciprocidad, familiaridad o compromiso social.

REQ 7.2 KPIs de capacidad de detección y respuesta

- **Tasa de reporte de amenazas.** Porcentaje de comunicaciones reales correctamente reportadas como sospechosas a través del mecanismo de reporte integrado.
- **Tiempo medio de reporte.** Tiempo transcurrido desde la recepción de la comunicación hasta su reporte como sospechosa.
- **Ratio de falsos positivos en reporte.** Porcentaje de comunicaciones legítimas reportadas erróneamente como sospechosas.
- **Tiempo medio de veredicto.** Tiempo transcurrido desde la recepción de la señal hasta la emisión de la clasificación final por parte de la plataforma.
- **Calidad del reporte.** Evaluación de la información proporcionada en el reporte: categorización correcta del tipo de amenaza, descripción de los indicadores de sospecha identificados y nivel de urgencia asignado.

REQ 7.3 KPIs de evolución y tendencia

- **Tendencia del índice de riesgo.** Evolución del índice en el tiempo, con identificación de puntos de inflexión, tendencias sostenidas de mejora o deterioro y correlación con eventos relevantes.
- **Velocidad de reducción del riesgo.** Tiempo medio que tarda una identidad o unidad operativa en reducir su índice de riesgo un nivel.
- **Cobertura de observación.** Porcentaje de identidades activas de la organización que están cubiertas por al menos un canal integrado durante el periodo de medición. Una cobertura inferior al 100% implica puntos ciegos en la observación del riesgo.



- **Frecuencia de análisis.** Número medio de señales procesadas por identidad y periodo, desglosado por canal.
- **Estabilidad del comportamiento.** Varianza del índice de riesgo de cada identidad en el tiempo. Una alta varianza indica comportamiento inconsistente; una baja varianza con índice bajo indica una reducción sostenida del riesgo.

REQ 7.4 KPIs de benchmarking y contexto

- **Benchmarking sectorial.** Comparación del índice de riesgo organizacional con los valores medios anonimizados de organizaciones del mismo sector, tamaño y geografía.
- **Benchmarking interno entre unidades operativas.** Ranking comparativo del índice de riesgo de las distintas unidades operativas, departamentos o divisiones.
- **Impacto económico estimado del riesgo.** Se valorará que la plataforma ofrezca un modelo de cuantificación económica del riesgo alineado con metodologías reconocidas como FAIR.
- **Correlación multicanal.** Análisis cruzado del comportamiento de cada identidad a través de todos los canales integrados, identificando patrones de exposición diferenciados.

REQUISITOS DE MOTOR DE GENERACIÓN DE INFORMES Y ANALÍTICA AVANZADA

REQ 8.1 Dashboards operacionales

La plataforma proporcionará dashboards operacionales en tiempo real con tres niveles de visualización:

Nivel de identidad individual. Vista completa del perfil de riesgo de cada identidad: índice actual y su evolución temporal, historial de comunicaciones analizadas y su clasificación, desglose por canal, técnicas de ingeniería social observadas, acciones ejecutadas, tasa y calidad de reporte, y posición relativa dentro de su unidad operativa.

Nivel de unidad operativa. Vista agregada del riesgo por departamento, división o unidad de negocio: índice de riesgo medio, distribución de identidades por tramos de riesgo, canales de mayor exposición, tendencia temporal, comparativa con otras unidades operativas y detalle de las identidades de riesgo persistente dentro de la unidad.

Nivel organizacional. Vista ejecutiva del programa: índice de riesgo organizacional y su evolución, cobertura de observación, principales áreas de riesgo, benchmarking sectorial, impacto acumulado de las acciones y proyecciones basadas en las tendencias observadas.

REQ 8.2 Informes automatizados

La plataforma permitirá configurar la generación y distribución automática de informes con periodicidad configurable (semanal, mensual, trimestral, anual). Los informes se distribuirán por correo electrónico a listas de destinatarios configurables y podrán adaptarse a diferentes audiencias: informes técnicos detallados para el equipo de seguridad, informes ejecutivos de alto nivel para el Comité de Dirección, e informes de cumplimiento para áreas de auditoría y gobernanza.



Todos los informes incorporarán la **imagen corporativa del cliente** (logotipo, colores, tipografía) y podrán exportarse en formato PDF con maquetación profesional y en formato CSV para análisis en herramientas externas.

REQ 8.3 Analítica avanzada e inteligencia artificial

Se valorará que la plataforma incorpore capacidades de analítica avanzada basada en inteligencia artificial, incluyendo:

- **Análisis predictivo:** identificación de patrones de deterioro del comportamiento que anticipen un incremento del riesgo antes de que se materialice, permitiendo intervenciones preventivas.
- **Segmentación automática:** agrupación de identidades en clusters de riesgo con comportamientos similares, identificando perfiles tipo que permitan diseñar estrategias de reducción del riesgo diferenciadas.
- **Detección de anomalías:** identificación de cambios bruscos en el patrón de comunicaciones o en la exposición de identidades individuales que puedan indicar compromiso real, insider threat o campañas activas.
- **Análisis de causa raíz:** identificación de los factores subyacentes que explican el riesgo conductual en la organización — ¿es un problema de susceptibilidad a la urgencia? ¿de exceso de confianza en comunicaciones internas? ¿de desconocimiento de los canales de verificación? — proporcionando inteligencia accionable para la dirección de seguridad.

REQUISITOS REQUISITOS TÉCNICOS DE LA PLATAFORMA

REQ 9 Requisitos técnicos de la plataforma

La plataforma dispondrá de una arquitectura **multitenant** con aislamiento completo de datos entre organizaciones, divisiones o unidades de negocio. La gestión del ciclo de vida de las identidades — alta, baja y modificación — se realizará de forma manual, mediante importación CSV y por **integración nativa con Microsoft Active Directory, Azure AD y Google Workspace** con sincronización automática. Se valorará el soporte de aprovisionamiento y desaprovisionamiento automatizado mediante protocolo **SCIM 2.0**.

La autenticación se resolverá mediante **Single Sign-On (SSO)** con soporte para SAML 2.0 y OpenID Connect, con delegación de la autenticación multifactor (MFA) al proveedor de identidad corporativo. El **control de acceso basado en roles (RBAC)** contemplará como mínimo tres roles diferenciados: administración completa, gestión operativa de campañas y acceso de solo lectura para auditoría.

Se requiere que la plataforma ofrezca la capacidad de **despliegue on-premise** mediante contenedores Docker con orquestación Kubernetes, en la infraestructura del cliente o cloud privado, con funcionalidad completa equivalente a la versión SaaS.

La arquitectura garantizará **escalado automático** horizontal y vertical con **balanceo de carga**, health checks y failover transparente. Se mantendrán **ambientes separados** de staging y producción con control de acceso independiente.

La política de **backups** contemplará copias diarias con retención de 90 días, semanales con retención de 3 meses y mensuales con retención de 9 meses, con replicación geográfica en una segunda ubicación. La gestión de copias de seguridad se realizará conforme a las directrices del NIST SP 800-209.



El **cifrado** de datos en reposo se realizará mediante AES-256-GCM y los datos en tránsito se protegerán con TLS 1.2 como versión mínima. Los módulos criptográficos empleados estarán validados conforme al estándar **FIPS 140-3**.

El proveedor garantizará un **SLA de disponibilidad** mínimo del 99,9%, con ventanas de mantenimiento programadas fuera de horario laboral y notificación anticipada mínima de 72 horas.

La plataforma expondrá una **API REST** completa con autenticación por token, cifrado SSL/TLS, documentación y entorno sandbox disponible para pruebas de integración.

Se exigirán conectores nativos con herramientas de **Business Intelligence** — al menos dos de las siguientes: Tableau, Power BI, Looker o IBM Cognos — para permitir la incorporación de los datos de riesgo conductual en los cuadros de mando analíticos de la organización. Se dispondrá de canal de comunicación operativa a través de **Microsoft Teams, Slack o Google Chat**.

Se valorará la integración con plataformas de **gestión de capital humano** (SAP SuccessFactors, Workday o Meta4) para la exportación de datos de desempeño, con **Microsoft Defender for Office 365** para el tratamiento automatizado de comunicaciones reportadas, y con plataformas **SIEM** (Splunk, QRadar u equivalentes) para correlación de eventos de seguridad.

El cumplimiento con el **RGPD** y la LOPDGDD será demostrable, con Acuerdo de Tratamiento de Datos (DPA) conforme al artículo 28 del RGPD. Las prácticas de **desarrollo seguro** seguirán las directrices OWASP Top 10 y OWASP ASVS, con revisión de código automatizada y análisis SAST/SCA integrados en el pipeline CI/CD. El proveedor realizará **pruebas de penetración externas** con periodicidad semestral, ejecutadas por empresa independiente acreditada, con informes disponibles bajo NDA.

La plataforma implementará controles de **prevención de fuga de datos (DLP)**, **WAF**, protección anti-DDoS y API Gateway con throttling, validación de esquemas y logging completo.

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

No Aplica

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Periodo de vigencia del licenciamiento ofertado: **36 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
Todas las licencias ofertadas	<ul style="list-style-type: none">• Derecho de uso: <i>por usuario</i>.• Derecho de actualización: <i>parches de seguridad, versiones menores, versiones mayores</i>,• Derecho de acceso a documentación: <i>documentación y manuales del fabricante</i>• Derecho de consulta al fabricante (soporte del fabricante):<ul style="list-style-type: none">○ Horario: <i>24x7x365</i>○ Tiempo de respuesta: <i>menos de 4 horas</i>○ Otros aspectos: <i>Revisiones de soporte mensuales, Revisiones trimestrales de operación, revisión anual de estado</i>



	<ul style="list-style-type: none">Otros derechos: <i>Technical support manager asignado por parte del fabricante</i>
--	--

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

Conforme al apartado III.2.3 del Pliego de Prescripciones Técnicas, las siguientes medidas¹⁰ 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: Haga clic o pulse aquí para escribir texto.
 - Responsable de la configuración de seguridad: Elija un elemento.

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.

¹⁰ 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

No aplica

II.2. SERVICIOS DE SOPORTE DE LOS PROGRAMAS A SUMINISTRAR

No aplica

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 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, limitando parcialmente la operativa, sin suponer la caída total del servicio.*
- *Severidad 3 (Leve): Incidencias menores sin impacto significativo en la seguridad o funcionalidad.*

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

II.2.2. ACUERDOS DE NIVEL DE SERVICIO

Se podrán dimensionar el servicio con los ANS que resulten más adecuados a la metodología de medición y/o sistema, según determine el organismo.

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. No se considerará el incorrecto desempeño del contratista por incumplimiento de los ANS si las incidencias superan el dimensionamiento del servicio previstos en el apartado anterior.

Cuando la resolución de la incidencia requiera la realización de desarrollos que por su naturaleza necesitan de un plazo material superior al indicado en la tabla precedente, el contratista estará obligado a presentar al Responsable del Contrato Específico en el organismo destinatario, dentro del plazo de tiempo de resolución inicial, un plan de actuación que incluya la duración prevista de los trabajos para la resolución, la justificación de dicha previsión y la descripción de los trabajos a realizar. Si es necesario, se incluirá la descripción de las medidas paliativas a adoptar hasta la completa resolución de la incidencia. Dicho plan deberá ser aprobado por el Responsable del Contrato Específico.

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: **1018620018705260308196**

ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

Contratos previos asociados con la instalación existente:

Contrato	Fecha adjudicación	Importe	Objeto
ACR-013-2026	24-02-2026	14.516,13	<i>Servicio de concienciación en ciberseguridad para evaluar el comportamiento usuario, identificar mejoras del factor humano y fortalecer la prevención frente a ingeniería social en entidades locales madrileñas</i>

La Agencia de Ciberseguridad de la Comunidad de Madrid dispone actualmente de una solución tecnológica **implantada y en explotación** (plataforma **ZEPO**) como resultado del contrato **ACR-013-2026**, adjudicado con fecha 24 de febrero de 2026.

El presente contrato tiene por objeto el suministro de licencias de acceso a una plataforma software de ciberseguridad orientada a la **detección, análisis y gestión del riesgo de ciberseguridad asociado a los canales de comunicación**. A estos efectos, la solución actualmente implantada constituye la **base tecnológica** sobre la que ya se encuentran desplegados e integrados (entre otros) configuraciones, conectores, modelos de medición, paneles e indicadores, así como series históricas de métricas.

Aunque el contrato previo tenía un componente de concienciación, **la exigencia de compatibilidad en este expediente no se fundamenta en necesidades formativas**. En la presente licitación **no** se pretende la prestación de servicios de formación, entrenamiento o sensibilización de usuarios, ni la ejecución de campañas formativas. La compatibilidad se exige **exclusivamente** para asegurar la **continuidad operativa**, la **continuidad metodológica** y la **comparabilidad** de las métricas e indicadores ya implantados, sin discontinuidades en la serie histórica.

Necesidad de un producto concreto. De conformidad con lo indicado en el Anexo I (REQ 0) y en el presente anexo, el suministro objeto del contrato deberá corresponder a la plataforma **ZEPO** o, en su caso, a una solución **equivalente únicamente en la medida en que garantice la compatibilidad técnica** con la solución implantada y la **continuidad metodológica** y **comparabilidad** de las métricas e indicadores ya existentes.

Definición de equivalencia (a efectos de este contrato). A los efectos de este contrato, se entenderá por “solución equivalente” aquella que, además de cubrir los requisitos funcionales del Anexo I, acredite de forma objetiva que permite:

- **Continuidad operativa** sin necesidad de una reimplantación completa de la solución.
- **Reutilización** de la configuración existente (parámetros, modelos de medición, reglas, taxonomías, cuadros de mando e integraciones) o, en su defecto, su migración con correspondencia trazable y sin pérdida funcional.



- **Preservación de la serie histórica** de métricas ya recopiladas (exportación/importación o mecanismo equivalente) sin pérdida de información relevante y manteniendo la misma semántica de datos.
- **Continuidad metodológica y comparabilidad** de indicadores: el cálculo de métricas e indicadores deberá mantenerse o, en caso de cambios, aportar un mapeo y justificación que garantice la comparabilidad con el histórico.
- **Interoperabilidad** con los conectores/API ya disponibles en la solución implantada o, alternativamente, la posibilidad de mantener las integraciones existentes sin rediseño integral.

Evidencias mínimas de compatibilidad (para soluciones equivalentes). En caso de ofertarse una solución equivalente a ZEPO, el licitador deberá incluir en su oferta técnica, como mínimo:

- Una **declaración del fabricante** o documentación oficial que describa la compatibilidad/mecanismo de migración aplicable a la situación descrita en este anexo.
- Una **descripción del procedimiento de transición**, incluyendo alcance, supuestos, dependencias, riesgos y medidas de mitigación.
- Una **matriz de correspondencia** entre métricas/indicadores existentes y los de la solución ofertada, indicando preservación, equivalencia o transformación.
- Un **plan de preservación del histórico** (exportación/importación, conservación, retención y verificación) que garantice la continuidad de series históricas y su comparabilidad.
- Un **inventario de integraciones** afectadas (conectores, API, sistemas terceros) y el modo en que se mantendrán sin interrupciones relevantes del servicio.

Justificación técnica y de eficiencia. La sustitución por una herramienta no compatible implicaría, entre otros efectos:

- La **redefinición y recalibración** de modelos de medición e indicadores, con impacto directo sobre la comparabilidad con el histórico.
- La necesidad de **validaciones funcionales y analíticas adicionales** para demostrar equivalencia de resultados y criterios de cálculo.
- Un **riesgo técnico y organizativo** asociado a la transición, incluyendo posible pérdida o degradación de series históricas.
- Un **impacto negativo en plazos** y en la continuidad de la medición, al requerir reconfiguración y ajuste de integraciones.

Desde el punto de vista de la **eficiencia en la gestión de los recursos públicos**, la compatibilidad con la solución implantada permite aprovechar configuraciones ya desarrolladas, evitar duplicidades de costes y preservar la continuidad de la medición, garantizando la trazabilidad y comparabilidad de la información generada.

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



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**

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



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**

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: 1018620018705260308196

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.¹¹
- **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

¹¹ 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/Doña, DNI, como Consejero Delegado/Gerente/ de la entidad, con NIF, y domicilio fiscal en

..... que participa como contratista/subcontratista en el desarrollo de actuaciones necesarias para la consecución de los objetivos definidos en el Componente XX

«.....»,

Efectúa las siguientes **DECLARACIONES**

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

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

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

- i. El nombre del perceptor final de los fondos;
- ii. el nombre del contratista y del subcontratista, cuando el perceptor final de los fondos sea un poder adjudicador de conformidad con el Derecho de la Unión o nacional en materia de contratación pública;
- iii. los nombres, apellidos y fechas de nacimiento de los titulares reales del perceptor de los fondos o del contratista, según se define en el artículo 3, punto 6, de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo (26);
- iv. una lista de medidas para la ejecución de reformas y proyectos de inversión en el marco del plan de recuperación y resiliencia, junto con el importe total de la financiación pública de dichas medidas y que indique la cuantía de los fondos desembolsados en el marco del Mecanismo y de otros fondos de la Unión».

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

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



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

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

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

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

Acredita la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT (declaración censal 036 o 037¹² 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:

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

¹² 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.

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

En todos los contratos específicos financiados¹³ por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiados, estableciéndose las siguientes **obligaciones**:

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

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

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

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

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

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

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

¹³ O es susceptible de ser financiado en caso de no haberse aún confirmado la selección por las autoridades correspondientes.



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.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**

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).



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1018620018705260308196**