

**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 para la continuidad y ampliación  
de la solución de arquitectura en la nube ‘Secure Access  
Service Edge – SASE’ para el servicio madrileño de salud,  
en el marco del PRTR, co-financiado por la unión europea  
– NextGenerationEU”

Lote 4 - Software de ciberseguridad

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



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962924269294671032772**

## TÉRMINOS Y CONDICIONES

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



10.2.	Condiciones de presentación de las facturas.....	19
11.	GARANTÍA DE LOS BIENES .....	19
12.	PENALIDADES .....	20
12.1.	Penalidades fijadas en el sistema dinámico de adquisición.....	20
12.2.	Fórmula para la aplicación de penalidades.....	21
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO .....	21
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS.....	21
	ANEXO I PRESCRIPCIONES TÉCNICAS.....	24
I.1.	Requisitos funcionales de los programas a suministrar .....	24
I.2.	Requisitos no funcionales de los programas a suministrar .....	29
I.3.	Periodo de vigencia y modalidad de licenciamiento .....	29
I.4.	Requisitos de seguridad de los programas en la nube .....	30
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO .....	30
II.1.	Servicios de instalación avanzada de los programas a suministrar.....	30
II.2.	Servicios de soporte de los programas a suministrar .....	30
II.2.1.	Dimensionamiento del servicio .....	32
II.2.2.	Acuerdos de nivel de servicio .....	32
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.....	37
	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 .....	45
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea.....	45
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR.....	47



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: 0962024269294671032772

## 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](mailto: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 para la continuidad y ampliación de la solución de arquitectura en la nube ‘Secure Access Service Edge – SASE’ para el servicio madrileño de salud, en el marco del PRTR, co-financiado por la unión europea – NextGenerationEU”**

### Objeto del contrato:

El objeto del presente contrato específico, derivado del Sistema Dinámico de Adquisición SDA 25/2022, es el suministro de licencias de una solución de arquitectura de ciberseguridad en la nube (Secure Access Service Edge – SASE), para el Servicio Madrileño de Salud, en el marco del PRTR cofinanciado por la unión europea-EU, y dentro del proyecto C15.I07.P06 - Programa de Impulso a la Industria de la Ciberseguridad Nacional y la actuación L4-Programa de refuerzo de la estrategia regional de ciberseguridad con la finalidad de:

- Garantizar la continuidad del servicio actualmente implantado
- Ampliar el número de usuarios protegidos mediante la incorporación de nuevas licencias.

### 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 invitación<sup>1</sup>. Los programas objeto del presente contrato específico, que forman parte de la arquitectura de seguridad del organismo destinatario son los siguientes<sup>2</sup>:

Todos los enumerados en el Anexo I de prescripciones técnicas

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

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

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

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

<sup>1</sup> 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.

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



- ☐ 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 entrega<sup>3</sup>: 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 del suministro, en las condiciones del apartado IV.2 del PPT, en el plazo<sup>4</sup> de 30 días hábiles, incluido el plazo de entrega de las licencias.
- ☐ El contrato incluye el servicio de instalación avanzada, a prestar por el adjudicatario, descrito en el **Anexo II** apartado 1. El plazo de ejecución de este servicio incluye el plazo para la entrega de las licencias y para la instalación y configuración básica.
- Plazo de ejecución: 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:

<sup>3</sup> Por defecto, 15 días naturales. El organismo podrá indicar un plazo superior.

<sup>4</sup> 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.





- 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 (€)
2.649.174,49 €	556.326,64 €	3.205.501,13 €

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
<b>SUMINISTRO</b>			
Suministro de licencias (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	2.598.535,86 €	545.692,53 €	3.144.228,39 €
<b>SERVICIOS</b>			
Servicio de instalación avanzada, a prestar por el adjudicatario			
Servicio de soporte, a prestar por el adjudicatario	50.638,63 €	10.634,11 €	61.272,74 €
Modificación prevista 20% (Estimación)			
<b>TOTAL</b>	<b>2.649.174,49 €</b>	<b>556.326,64 €</b>	<b>3.205.501,13 €</b>

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 suplirá el importe máximo del contrato específico.

En todo caso, el importe de los servicios deberá ser inferior al importe de los suministros. Asimismo, cada uno de los conceptos presupuestarios desglosados en la tabla anterior (suministro de licencias, instalación avanzada y/o soporte) opera como límite máximo de gasto, por lo que las ofertas no deberán superar el importe de ninguno de ellos, incluso aunque el





importe total de la oferta en su conjunto sea inferior al presupuesto base de licitación. Serán excluidas del procedimiento las ofertas que no se adecuen a estas estipulaciones.

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

Aplicación presupuestaria	Anualidad 2026	Anualidad 2027	TOTAL
Suministro de licencias para la continuidad y ampliación de la solución de arquitectura en la nube 'Secure Access Service Edge – SASE' para el servicio madrileño de salud.	3.190.182,94 €	15.318,18 €	3.205.501,13 €

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

	Fondos	Anualidad 2026	Anualidad 2027	Total
Fondos RETECH	98,57%	2.611.195,52 €		2.611.195,52 €
Fondos Propios	1,43%	25.319,31 €	12.659,66 €	37.978,97 €
IVA		553.668,11 €	2.658,53 €	556.326,64 €
		3.190.182,94 €	15.318,18 €	3.205.501,13 €

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	45.213,06 €
Resto costes directos	2.320.121,30 €
<b>Costes indirectos + Gastos generales + Beneficio industrial</b>	<b>283.840,12 €</b>
<b>Total sin IVA</b>	<b>2.649.174,49 €</b>

Justificación: El objeto del contrato es la adquisición de unas licencias de software, así como la prestación de servicios adicionales de soporte personalizado. Esto implica que los costes directos abarcan la totalidad de los gastos asociados a la adquisición de la licencia y la prestación de los servicios mencionados, 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.

Si en el apartado 2 se ha indicado que se solicitan servicios a prestar por el adjudicatario, es de aplicación lo siguiente:

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

El convenio colectivo sectorial de aplicación en los términos indicados es el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública, publicado en el BOE del día 16 de abril de 2025 mediante Resolución de 4 de abril de 2025, de la Dirección General de Trabajo, por la que se registra y publica el citado Convenio. No consta que exista diferencia por género en el Convenio colectivo que resulta de aplicación.

Costes de personal							
Perfiles	Dedicación	Salario Base	Especialización tecnológica (XX%) <sup>5</sup>	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 30%
PO SASE (Project Manager TI)	50%	31.138,47 €	<b>110%</b>	34.252,32 €	17.126,16 €	17.126,16 €	22.606,53 €
Técnico Monitoreo / Gestor Ops Continuo Optimización diaria	50%	31.138,47 €	<b>110%</b>	34.252,32 €	17.126,16 €	17.126,16 €	22.606,53 €
							<b>45.213,06 €</b>

Si bien resulta de aplicación el Convenio sectorial, en el presente servicio se requiere una cualificación superior debido a la especialización tecnológica requerida y al bajo número de recursos en el mercado especializados en este tipo de tecnologías. Dicha columna de

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



especialización se ha consignado tomado como referencia los salarios actuales del mercado y el informe de la consultora Hays 2025, sobre costes laborales.

Este informe refleja los precios de mercado de diferentes perfiles laborales dentro de varios sectores de actividad industrial. Para este contrato se ha tomado como referencia en Área 5 de Ciberseguridad, por ello que se requieren de los coeficientes por especialización tecnológica que se reflejan en la tabla anterior.

#### 4.3. TRAMITACIÓN DEL EXPEDIENTE (A EFECTOS PRESUPUESTARIOS)

☒ Ordinaria.

☐ Anticipada:

Se hace constar que el plazo de ejecución comenzará a partir del **1 de enero de 202X o fecha posterior**, y que la adjudicación del contrato queda sometida a la condición suspensiva de existencia de crédito adecuado y suficiente para financiar las obligaciones derivadas del contrato en el ejercicio correspondiente, de acuerdo con el artículo 117.2 de la LCSP y la normativa contable de aplicación.

#### 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 específico<sup>6</sup>:
  - No aplica

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

#### 4.5. VALOR ESTIMADO

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



Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **DOS MILLONES SEISCIENTOS CUARENTA Y NUEVE MIL CIENTO SETENTA Y CUATRO EUROS CON CUARENTA Y NUEVE CÉNTIMOS euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	2.649.174,49 €
Importe máximo por modificación prevista, sin IVA	Haga clic o pulse aquí para escribir texto.
<b>TOTAL</b>	<b>2.649.174,49 €</b>

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 PONDERACIÓN<sup>7</sup>

### 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
N/A	N/A	N/A

<sup>7</sup> Criterios de valoración conforme a las previsiones del apartado 27.5.4 del PCAP.



## 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**:

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

Donde:

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

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



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: 0962024269294671032772

**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 RGPD<sup>8</sup>.

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.

<sup>8</sup> 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>.



☐ Otra: Especificar...

## 10.2. CONDICIONES DE PRESENTACIÓN DE LAS FACTURAS

☐ Organismo incluido en el ámbito subjetivo, art 229.2 LCSP.

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

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

- Órgano de contratación: Dirección General de Racionalización y Centralización de la Contratación - E04962703.
- Órgano responsable del contrato específico (DIR3): Haga clic o pulse aquí para escribir texto.
- Órgano gestor (DIR3): Haga clic o pulse aquí para escribir texto.
- Unidad tramitadora (DIR3): Haga clic o pulse aquí para escribir texto.
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3): Haga clic o pulse aquí para escribir texto.

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

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

☒ Organismo adherido al Sistema Estatal de Contratación Centralizada.

*La Agencia de Ciberseguridad de la Comunidad de Madrid gestionará, las facturas recibidas en el "Punto General de Entrada de Facturas Electrónicas", FACe, en los términos establecidos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y sus disposiciones de desarrollo. En las facturas deberán constar los siguientes datos, de conformidad con lo dispuesto en la disposición adicional trigésima segunda de la LCSP: • Órgano de contratación: Agencia de Ciberseguridad de la Comunidad de Madrid – Q2802867H. • Código DIR3: El código único para el órgano gestor, la unidad tramitadora y la oficina contable es el A13050393. Asimismo, en el formato electrónico de la factura se debe incluir en el campo ReceiverTransactionReference el valor ACR-009-2026.*

## 11. GARANTÍA DE LOS BIENES

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



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

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

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

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

## 12. PENALIDADES

### 12.1. PENALIDADES FIJADAS EN EL SISTEMA DINÁMICO DE ADQUISICIÓN

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

	Valor fijado en el SDA	Valor fijado en el contrato específico	Fórmula de cálculo
Incumplimiento de las condiciones especiales de ejecución, excepto las relativas a subcontratación.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo	<i>No Aplica</i>	N/A
Incumplimiento de los compromisos de adscripción de medios.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas.	2% de la facturación del periodo	<i>No Aplica</i>	Apartado 12.2
Demora en el cumplimiento del plazo total del contrato	Resolución / 0,60 euros por cada día y 1.000 euros del precio del contrato, IVA excluido		Valor fijado en el SDA
Incumplimiento de obligaciones en materia medioambiental, social o laboral	2% de la facturación del periodo		Apartado 12.2
Incumplimiento de las condiciones de subcontratación	2% del importe del subcontrato <i>Grave: 5%</i> <i>Muy grave: 10%</i>		Valor fijado en el SDA



Incumplimiento de las obligaciones de información y pago sobre suministradores y subcontratistas.	2% del importe del subcontrato <i>Grave: 5%</i> <i>Muy grave: 10%</i>	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 PLACSP<sup>9</sup> u otra plataforma de contratación a disposición del organismo.

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





Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa<sup>10</sup>.

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:

[https://contratacioncentralizada.gob.es/documents/32143/48667/Modelos+de+Oferta+SDA25\\_2022.zip/b255fa33-a721-b657-d308-743f00fb56b4?t=1759159939180](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
- 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/>

---

<sup>10</sup> 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.





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](mailto:licita_agencia_ciber@madrid.org)

Con la finalidad de dar cumplimiento a las medidas destinadas a las entidades adheridas para velar por la correcta aplicación de los términos, condiciones e instrucciones que regulan el Sistema Dinámico de Adquisición de suministro de software de sistema, de desarrollo y de aplicación (SDA 25/2022), los pliegos rectores del SDA se encuentran disponibles en el siguiente enlace: [https://contrataciondelestado.es/wps/wcm/connect/2e5cb41d-d508-4a7f-ae25-c5f986492db9/DOC\\_CD2022-214850.pdf?MOD=AJPERES](https://contrataciondelestado.es/wps/wcm/connect/2e5cb41d-d508-4a7f-ae25-c5f986492db9/DOC_CD2022-214850.pdf?MOD=AJPERES)

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

EN LO QUE ESTE DOCUMENTO DE INVITACIÓN SE OPONGA A LOS PLIEGOS DEL SISTEMA DINÁMICO DE ADQUISICIÓN, 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):** Haga clic o pulse aquí para escribir texto.

**Firmado electrónicamente (nombre y apellidos):** Haga clic o pulse aquí para escribir texto.



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962924269294671032772**

## ANEXO I PRESCRIPCIONES TÉCNICAS

### I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

*Se requiere la adquisición de una solución de ciberseguridad ZTNA basada en la nube para asegurar la conectividad de los usuarios a las aplicaciones privadas con un modelo de arquitectura Zero Trust completa. El objetivo es optimizar la gestión de seguridad, garantizar el acceso seguro de los usuarios, eliminando la superficie de ataque en internet a la vez que se suprimen los riesgos de movimiento lateral, y fortalecer la capacidad de respuesta ante amenazas emergentes.*

*A continuación, se detallan los requerimientos técnicos obligatorios del suministro:*

Referencia	Programa	Cantidad
Zscaler Private Access Platform o equivalente	ZS-ZPA-PLATFORM	14.000
Zscaler Data Protection Browser Isolation Advanced o equivalente	ZS-DP-ISO-ADV	14.000
Zscaler Private Access o equivalente	ZS-ZPA-2	14.000
Zscaler Support Plus o equivalente	ZCES-SUP-PLUS	1

*Con carácter excepcional, habiendo justificado de manera motivada la existencia de razones objetivas que imposibilitan hacerlo de la manera anterior, se autorizará tal referencia, acompañada obligatoriamente de la mención “o equivalente”.*

*Asimismo, cuando las prescripciones técnicas se formulen haciendo referencia a normas internacionales o a otros sistemas de referencias técnicas elaborados por los organismos europeos de normalización o a normas nacionales (normas UNE, EN, ISO), deberán ir acompañadas del término “o equivalente”, salvo que existan instrucciones o reglamentos técnicos nacionales que exijan la norma obligatoriamente, en cuyo caso se recomienda citar en el documento de invitación o en la memoria, la instrucción o reglamento técnico nacional que habilita la excepción en este supuesto.*

*En los dos casos anteriores, se indicará que la equivalencia debe entenderse en los términos que define el apartado III.1 del Pliego de Prescripciones Técnicas.*

#### A. Requerimientos funcionales y de arquitectura (ZTNA)

**A1.- La solución DEBE proporcionar Zero Trust Network Access (ZTNA) con control de acceso por aplicación (no por red/subred/VLAN).**

**A2.- La solución DEBE soportar todo tipo de aplicaciones: web (HTTP/HTTPS), cliente/servidor (TCP), protocolo UDP, limitando siempre a aplicaciones explícitamente autorizadas.**

**A3.- La solución DEBE soportar comunicación con las aplicaciones a través de protocolo ICMP. La solución por tanto DEBE permitir realizar ping o traceroute a los servidores y aplicaciones destino a través de la solución ZTNA para testeo de las comunicaciones. No se consideran válidas alternativas como el uso de nslookup, tcping psping u otras herramientas basadas en TCP.**

*A4, La solución DEBE evitar la exposición de aplicaciones y servicios privados a Internet (sin publicación directa, sin reglas de acceso hacia las aplicaciones desde Internet).*

*A5, La solución DEBE soportar un modelo inside-out donde los componentes desplegados en el entorno del cliente establecen únicamente conexiones salientes hacia el servicio.*

*A6, La solución DEBE impedir el movimiento lateral, no otorgando conectividad de red general (sin rutas amplias) y evitando descubrimiento de servicios no autorizados.*

*A7, La solución DEBE permitir microsegmentación y políticas granulares por identidad (usuario/grupo), aplicación, FQDN/host, puerto, protocolo, y contexto.*

*A8, La solución DEBE soportar segmentación por entorno (prod/preprod/dev) y por tipo de usuario (empleado/tercero) mediante políticas separadas.*

*A9, La solución DEBE soportar despliegue distribuido en múltiples centros de datos on-premise y en infraestructuras cloud como Azure y AWS, manteniendo una política consistente global.*

*A10, La solución DEBE soportar despliegue en multicloud con el mismo modelo operativo.*

*A11, La solución DEBE proporcionar alta disponibilidad por diseño mediante despliegue redundante de conectores/elementos de publicación por ubicación/entorno.*

*A12, La solución DEBE soportar un modelo de onboarding de aplicaciones rápido, sin rediseñar el direccionamiento ni extender la red a usuarios remotos.*

*A13, La solución DEBE permitir definir aplicaciones por FQDN (y/o IP/puerto cuando aplique) y agruparlas en “application segments” o equivalentes.*

**B. Identidad, autenticación y políticas (Entra ID)**

#### **#, Requerimiento**

*B1, La solución DEBE integrarse con Microsoft Entra ID como IdP mediante estándares (SAML/OIDC) para SSO.*

*B2, La solución DEBE soportar MFA vía Entra ID y respetar Conditional Access (o controles equivalentes del IdP).*

*B3, La solución DEBE permitir políticas basadas en cualquier atributo de usuario/grupo provenientes de Entra ID.*

*B4, La solución DEBE soportar diferenciación de políticas para empleados vs. terceros (incl. reglas de autenticación y alcance de aplicaciones).*

*B5, La solución DEBE soportar integración con señales de riesgo/contexto (p.ej. ubicación, tipo de dispositivo, etc.) para decisiones adaptativas.*

**C. Acceso con agente (empleados / dispositivos gestionados)**

#### **#, Requerimiento**



*C1, La solución DEBE soportar un agente en puestos de usuario corporativos para habilitar acceso ZTNA a aplicaciones no web y web cuando aplique.*

*C2, El agente o cliente Software DEBE estar disponible para plataformas Windows, Linux, Mac, iOS y Android. Debe permitirse la configuración de perfiles de instalación diferentes para cada tipo de plataforma.*

*C3, La solución DEBE permitir políticas condicionadas a postura del dispositivo (device trust/compliance) para acceso a aplicaciones sensibles. Entre los criterios a aplicar para determinar la postura de seguridad del dispositivo deben estar incluidos al menos los siguientes:*

- *Existencia de certificado de confianza*
- *Existencia de fichero en un path concreto*
- *Existencia de Clave de Registro*
- *Certificado cliente*
- *Certificado cliente con validación de servidor*
- *Versión de Sistema Operativo*
- *Detección de JAMF*
- *Estado del servicio de Firewall de Sistema*
- *Detección de antivirus habilitado en el puesto*
- *Cifrado de disco habilitado*
- *Dominio al que está unido el equipo*
- *Equipo unido a AzureAD Domain*
- *Chequeo de proceso en ejecución*
- *Detección de clientes EDR como Carbon Black, CrowdStrike, MS Defender o SentinelOne*
- *Nivel de riesgo dinámico ZTA de CrowdStrike*

*C4, La solución DEBE proporcionar acceso por aplicación sin configurar VPN ni conceder conectividad general a redes internas.*

*C5, La solución DEBE ofrecer herramientas de diagnóstico (estado del agente, prueba de acceso por aplicación, trazabilidad de decisión de política).*

*D. Acceso sin agente (terceros / BYOD)*

#### **#, Requerimiento**

*D1, La solución DEBE ofrecer acceso sin agente a aplicaciones web internas desde navegador, con SSO mediante Entra ID.*

*D2, La solución DEBE permitir que el acceso sin agente esté restringido por aplicación (no por red) y separado de empleados.*

*D3, La solución DEBE soportar la aplicación de métodos de Browser Isolation en el acceso a aplicaciones Web Privadas sin agente, como se indica más adelante.*



*D4, En ningún caso se aceptarán soluciones que requieran la instalación de un agente o un plugin o cualquier tipo de software para dar acceso a terceros.*

#### *E. SaaS de terceros + Isolation*

##### **#, Requerimiento**

*E1, La solución DEBE soportar acceso a aplicaciones SaaS de terceros con la capacidad de aplicar aislamiento de navegador (isolation) para reducir riesgo en navegación y acceso.*

*E2, La solución DEBE soportar el acceso a cualquier aplicación SaaS de terceros (no puede existir una lista restringida de aplicaciones accesibles) sin requerir la instalación de ningún software adicional.*

*E3, La solución DEBE permitir políticas por usuario/grupo y contexto para decidir cuándo aplicar isolation a SaaS (p.ej. terceros, dispositivos no gestionados, aplicaciones de riesgo).*

*E4, La solución DEBE registrar auditoría del acceso a SaaS y de la aplicación de isolation (quién, qué aplicación, cuándo, decisión de política).*

*E5, La solución DEBE otorgar control completo de la sesión, permitiendo el control (permitir/bloquear) de al menos las siguientes acciones: copiar/pegar texto, subir o descargar archivos, imprimir, e incluso insertar una marca de agua que permita identificar el contenido usuario, marca de tiempo y mensaje personalizable. No se admitirán soluciones que requieran la instalación de software, agente, o plugin para poder aplicar cualquiera de esos controles.*

#### *F. Observabilidad, auditoría y cumplimiento*

##### **#, Requerimiento**

*F1, La solución DEBE proporcionar logging centralizado de autenticación/autorización/acceso por aplicación (usuario, grupo, app, ubicación, dispositivo, resultado).*

*F2, La solución DEBE permitir exportación a SIEM (formato estándar y near real-time).*

*F3, La solución DEBE ofrecer trazabilidad de decisión de política (por qué se permitió/denegó).*

*F4, La solución DEBE soportar retención, búsqueda y reporting para auditorías.*

#### *G. Requerimientos de operación y resiliencia*

##### **#, Requerimiento**

*G1, La solución DEBE soportar HA por ubicación/entorno (N+1 o equivalente) y no depender de un único punto de fallo en cada DC/VNET.*

*G2, La solución DEBE soportar actualizaciones controladas de componentes (con ventanas, anillos/canary, rollback o mecanismos equivalentes).*

*G3, La solución DEBE soportar segregación administrativa (RBAC) y separación de funciones (admins de seguridad vs. operaciones).*



*G4, La solución DEBE proporcionar controles para asegurar que las apps privadas permanezcan no enrutables/no descubribles desde redes no autorizadas.*

#### *H. Requerimientos de Seguridad*

##### **#, Requerimiento**

*H1, La solución DEBE permitir configurar políticas de protección a nivel de aplicación (Layer 7) para inspeccionar tráfico de aplicaciones privadas HTTP/HTTPS y bloquear intentos de explotación, incluyendo como mínimo los siguientes controles:*

- *Open Web Application Security Project (OWASP)*
- *Últimas amenazas proporcionando controles actualizados escritos y mantenidos por el proveedor que protegen frente a nuevos vectores de ataque y vulnerabilidades emergentes.*
- *Protección de protocolo WebSocket*
- *Protección de API frente a las amenazas más recientes inspeccionando sus transacciones para detectar posibles violaciones de seguridad, y proveyendo de visibilidad detallada de los datos de la API (usuarios, métodos, errores y gestión de información confidencial)*
- *Protección de las aplicaciones internas de las últimas amenazas inspeccionando las transacciones de segmentos de aplicaciones habilitadas para Active Directory para detectar violaciones de seguridad, soportando el análisis de los protocolos Kerberos, SMB y LDAP.*
- *Inclusión de controles personalizados.*

*H2, La solución DEBE permitir crear y gestionar Perfiles de protección de aplicaciones (incluyendo niveles de sensibilidad/paranoia y controles predefinidos y/o personalizados) y asociarlos a políticas por aplicación para adaptar protección y reducir falsos positivos. Estos perfiles deben permitir elegir los controles a usar en cada perfil diferenciando entre Controles predefinidos de OWASP, controles personalizados, controles de frente a nuevas amenazas, controles de WebSocket, controles de API y controles de Active Directory*

*H3, La solución DEBE incluir de forma predefinida controles específicamente identificados para OWASP, identificando los controles asociados con cada versión (incluyendo al menos las versiones OWASP\_CRS/4.8.0 y OWASP\_CRS/3.3.5*

*H4, La solución DEBE permitir seleccionar de forma individual cada uno de los controles que se activan para cada perfil, así como seleccionar de forma individual en los perfiles la acción a realizar para cada control, permitiendo bloquear o únicamente monitorizar.*

*H5, La solución DEBE identificar cada control con el tipo de control al que se refiere (Nuevos ataques, OWASP en sus diferentes versiones, API Protection, Websocket Protection o Active Directory Protection) y debe permitir buscar y filtrar los controles predefinidos.*

*H6, La solución DEBE permitir añadir nuevos controles personalizados (custom) que podrán activarse de forma independiente para cada perfil de seguridad.*



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962024269294671032772**



H7, La solución DEBE incluir capacidad de Deception integrada mediante despliegue de estrategias y señuelos (decoys) para detectar reconocimiento, enumeración y actividad maliciosa relacionada con el acceso a aplicaciones privadas, generando alertas de alta fidelidad.

H8, La solución Deception DEBE estar plenamente integrada en la solución de acceso remoto seguro, siendo ofrecida por el mismo fabricante y permitiendo la creación de decoys o señuelos sobre la misma plataforma sin necesidad de desplegar ningún elemento en la red o infraestructura de SERMAS.

Todos los requerimientos incluidos en este apartado son de obligado cumplimiento, debiendo el proveedor acreditar que la solución cumple mediante enlace a la documentación pública o guía de configuración del proveedor que acredite el cumplimiento de los requerimientos.

La Agencia de Ciberseguridad se reserva el derecho de solicitar al proveedor una prueba de aceptación para validación de los criterios y requerimientos previamente expuestos.

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

No Aplica

## I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Vigencia de las licencias:

Programa	Periodo de vigencia del licenciamiento
Zscaler Private Access Platform o equivalente	36 meses
Zscaler Data Protection Browser Isolation o equivalente	36 meses
Zscaler Private Access o equivalente	36 meses
Zscaler Support Plus o equivalente	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
Zscaler Private Access Platform	<ul style="list-style-type: none"> <li>Derecho de uso: <i>por usuario</i>.</li> <li>Derecho de actualización: <i>parches de seguridad, versiones menores, versiones mayores</i>,</li> </ul>
Zscaler Data Protection Browser Isolation	<ul style="list-style-type: none"> <li>Derecho de acceso a documentación: <i>documentación y manuales del fabricante</i></li> </ul>
Zscaler Private Access	<ul style="list-style-type: none"> <li>Derecho de consulta al fabricante (soporte del fabricante): <ul style="list-style-type: none"> <li>Horario: <i>24x7x365</i></li> <li>Tiempo de respuesta: <i>menos de 4 horas</i></li> <li>Otros aspectos: <i>Revisiones de soporte mensuales, Revisiones trimestrales de operación, revisión anual de estado</i></li> </ul> </li> </ul>
Zscaler Support Essentials	





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

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

Conforme al apartado III.2.3 del Pliego de Prescripciones Técnicas, las siguientes medidas<sup>11</sup> 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.

### 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

##### Alcance

El adjudicatario prestará un servicio orientado a asegurar la **operación continuada y el mantenimiento ordinario** de la solución suministrada, incluyendo las actuaciones necesarias

<sup>11</sup> 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.



para su correcta utilización, estabilidad y disponibilidad en el entorno del Servicio Madrileño de Salud (SERMAS) y de la Agencia para la Administración Digital de la Comunidad de Madrid.

El servicio comprenderá aquellas actuaciones necesarias para que la solución se mantenga correctamente configurada, integrada y operativa, conforme a los requisitos de seguridad, rendimiento y cumplimiento normativo aplicables, dentro de los parámetros y configuraciones existentes, asumiendo el adjudicatario la responsabilidad sobre la adecuada prestación del soporte durante la vigencia del contrato.

La solución deberá dar servicio a un total de 14.000 usuarios, proporcionando acceso remoto seguro a aplicaciones privadas, conforme a los principios de seguridad por defecto, mínimo privilegio y confianza basada en el contexto.

### **Servicios incluidos**

Como parte del servicio de soporte y operación ordinaria, se incluirán, entre otras, las siguientes actuaciones:

- Mantenimiento y ajuste de la configuración funcional y técnica de la solución, garantizando su compatibilidad con los sistemas, plataformas y herramientas existentes en el organismo, así como su adecuación al Esquema Nacional de Seguridad, RGPD y demás normativa aplicable.
- Coordinación con los equipos de Madrid Digital y de Salud Digital para la operación y correcta integración de los elementos necesarios en los entornos del organismo, tanto en infraestructuras on-premise como en entornos Cloud.
- Parametrización y ajustes funcionales y técnicos de carácter menor en los distintos módulos, licencias y conectores de la solución, así como en sus integraciones con otros sistemas corporativos (SIEM, EDR u otros), con el fin de mantener su correcto funcionamiento.
- Mantenimiento de roles, perfiles, políticas de acceso y reglas operativas, en coordinación con los responsables del directorio corporativo, incluyendo el mapeo de usuarios y la aplicación de políticas basadas en autenticación y atributos.
- Aplicación de criterios de seguridad basados en el principio de privilegio mínimo y confianza contextual, considerando factores como la ubicación del usuario, la postura de seguridad del dispositivo, la aplicación solicitada y el tipo de información gestionada.
- Prestación de soporte funcional y técnico, incluyendo la atención a consultas, la gestión y resolución de incidencias conforme a criterios de severidad y acuerdos de nivel de servicio, así como la vigilancia del funcionamiento general de la plataforma.
- Monitorización del servicio y gestión de incidencias en modalidad 24x7, garantizando la trazabilidad de las actuaciones realizadas y la comunicación periódica con la Agencia sobre el estado y resolución de los eventos detectados.
- Elaboración y mantenimiento de documentación técnica y operativa, actualizada conforme a la evolución del servicio, relativa a la configuración, operación, administración y mantenimiento de la solución, de acuerdo con los procedimientos establecidos por la Agencia.



- Aplicación y mantenimiento de un procedimiento operativo de gestión de cambios, orientado a la gestión ordenada de altas, modificaciones o bajas de usuarios y permisos, así como a ajustes funcionales necesarios para la operación ordinaria de la solución. Dicho procedimiento deberá ser validado por el Responsable del Proyecto de la Agencia.
- Elaboración de informes periódicos de actividad, con detalle de incidencias gestionadas, tiempos de respuesta y resolución, actuaciones realizadas y observaciones operativas, que serán presentados en los comités de seguimiento correspondientes.

### Organización del servicio

El servicio será prestado por un equipo técnico cualificado y con experiencia acreditada en soluciones de características equivalentes. El adjudicatario designará un interlocutor técnico que actuará como punto de contacto con el Responsable del Proyecto designado por la Agencia y coordinará las actuaciones necesarias para la correcta prestación del servicio de soporte.

El adjudicatario será responsable de la interlocución con el fabricante de la solución, asegurando la correcta aplicación de las recomendaciones que resulten necesarias y comunicando a la Agencia cualquier incidencia relevante detectada durante la operación ordinaria del servicio.

#### 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



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962924269294671032772**

## 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: 0962924269294671032772

## ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

Contratos previos asociados con la instalación existente:

Contrato	Fecha adjudicación	Importe	Objeto
“SERVICIO DE SUSCRIPCIÓN A BASES DE DATOS ESPECIALIZADAS EN ACCESO REMOTO SEGURO PARA EL SERVICIO MADRILEÑO DE SALUD, CON CARGO AL PLAN DE RECUPERACIÓN TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA – FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU” <b>C11.I03.P14.S13</b>	<b>Noviembre- 2025</b>	202.911,86 € (impuestos excluidos)	SERVICIO DE SUSCRIPCIÓN A BASES DE DATOS ESPECIALIZADAS EN ACCESO REMOTO SEGURO PARA EL SERVICIO MADRILEÑO DE SALUD.

En la actualidad el Servicio Madrileño de Salud, dispone de una plataforma SASE-ZTNA del proveedor Zscaler, en régimen de derecho de uso, para dar cobertura de conectividad segura a los usuarios y sistemas del organismo.

La plataforma se encuentra plenamente implantada y en producción, integrada en sus sistemas corporativos, cuya sustitución implicaría elevados costes económicos, técnicos y operativos, así como riesgos significativos de interrupción del servicio, por lo que se justifica la referencia tecnológica por motivos de continuidad operativa, proporcionalidad y eficiencia.

La renovación y ampliación de licencias objeto del presente contrato específico resulta imprescindible para garantizar la continuidad del servicio de ciberseguridad, evitando riesgos operativos, de seguridad y de cumplimiento normativo.

El final del ciclo de vida de un producto o licencia es una vulnerabilidad conocida en ciberseguridad. Cuando una licencia expira o deja de ser soportada, deja de recibir actualizaciones de seguridad, parches y soporte técnico, lo que convierte al software en un objetivo fácil para los ciberataques.

Por lo tanto, la renovación de estas licencias no es solo una cuestión operativa, sino una medida esencial de ciberseguridad para mitigar los riesgos, asegurar la continuidad del negocio y garantizar el cumplimiento de las normativas de protección de datos.

La arquitectura actual se construyó, probó y optimizó específicamente para funcionar con las licencias y el software existente. Esto representa una inversión considerable en tiempo, dinero



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962924269294671032772**

y recursos humanos. Cambiar a un producto alternativo no es simplemente "instalar un nuevo software". Implica una migración completa de datos y configuraciones, reentrenamiento del personal, y una posible reestructuración de la infraestructura para asegurar la compatibilidad. Estos costes son directos y muy elevados. Durante la migración, existe un alto riesgo de interrupciones del servicio, pérdida de datos o fallos de seguridad no previstos. Esto podría comprometer la disponibilidad y la integridad de los sistemas críticos del SERMAS, un aspecto fundamental de la ciberseguridad. La arquitectura existente probablemente depende de funcionalidades específicas del producto actual. Sus API, protocolos de comunicación y modos de integración con otros sistemas de la empresa (como SIEM, IAM, etc.) son únicos. Un producto alternativo podría no tener las mismas características, lo que obligaría a reconfigurar o incluso reemplazar otros componentes de la arquitectura.

Al mantener el producto actual, la empresa se enfrenta a un conjunto de riesgos conocidos y gestionados. Se tienen procedimientos establecidos para aplicar parches, monitorear vulnerabilidades y responder a incidentes. Un nuevo producto, por muy bueno que sea, trae consigo un nuevo conjunto de riesgos desconocidos y vulnerabilidades que aún no han sido plenamente identificadas o gestionadas por la empresa.

En resumen, la justificación no se basa en que el producto alternativo sea peor, sino en el alto coste y el riesgo inherente al cambio. La renovación de las licencias actuales es la opción más segura, estable y económicamente viable para mantener la continuidad del negocio y el nivel de protección en ciberseguridad que ya se ha logrado con la arquitectura existente. Es una decisión estratégica que prioriza la estabilidad y la mitigación de riesgos sobre la adopción de una tecnología potencialmente nueva.

La sustitución de la tecnología existente implicaría elevados costes económicos, técnicos y operativos, así como riesgos significativos de interrupción del servicio, pérdida de integraciones y degradación de la postura de seguridad. Por ello, se justifica la referencia tecnológica por motivos de compatibilidad, continuidad operativa y eficiencia, conforme al artículo 126.6 de la LCSP.

La renovación de licencias existentes y la ampliación del número de usuarios se realizan como suministro recurrente de software, no constituyendo en ningún caso una prórroga contractual ni una modificación del contrato anterior, sino un nuevo contrato específico tramitado al amparo del Sistema Dinámico de Adquisición SDA 25/2022.





**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**

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

D./D<sup>a</sup>:....., con D.N.I. n<sup>o</sup>:....., actuando en nombre propio / en representación de (a empresa licitadora) ..... con N.I.F.:....., con domicilio (de la empresa licitadora) en (calle/plaza/etc.):....., n<sup>o</sup>:....., 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	



La autenticidad de este documento se puede comprobar en <https://gestiona.comunidad.madrid/csv> mediante el siguiente código seguro de verificación: 0962024269294671032772

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

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

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

(Fecha, firma y nombre completo del representante legal)

Fdo. electrónicamente



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

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

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: **0962924269294671032772**

## 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.<sup>12</sup>
- **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

<sup>12</sup> 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 037<sup>13</sup> 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: .....

<sup>13</sup> 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.







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

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

En todos los contratos específicos financiados<sup>14</sup> 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.

---

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



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

## **5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO**

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

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

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

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

## **7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN**

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

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

## **8. PROHIBICIÓN DE DOBLE FINANCIACIÓN**

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



La autenticidad de este documento se puede comprobar en  
<https://gestiona.comunidad.madrid/csv>  
mediante el siguiente código seguro de verificación: **0962924269294671032772**

## 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 si 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).

