

**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 DEL LICENCIAMIENTO DE LA PLATAFORMA
AUTOMATIZADA DE PRUEBAS DE PENTESTING Y GESTIÓN
DE SUPERFICIE DE ATAQUE INTERNA/EXTERNA EN EL
MARCO DEL PRTR, CO-FINANCIADO POR LA UNIÓN
EUROPEA – NEXTGENERATIONEU**

(Expediente Nº ACR-015-2026)

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: **1055154624058134589260**

TÉRMINOS Y CONDICIONES

1.	ORGANISMO DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO	5
2.	LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO	5
2.1.	Lote, título y objeto	5
2.2.	Características principales de las prestaciones	6
2.3.	Tratamiento de datos de carácter personal por parte del adjudicatario	6
2.4.	Categorización conforme al Esquema Nacional de Seguridad (ENS)	7
2.5.	Tratamientos de datos personales para los programas en modalidad de nube	7
3.	DURACIÓN DEL CONTRATO	8
3.1.	Fecha de inicio de la ejecución	8
3.2.	Plazo de entrega de las licencias	8
3.3.	Plazo de ejecución del contrato	9
3.4.	Prórroga del contrato específico	9
4.	VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN	9
4.1.	Presupuesto de licitación y aplicaciones presupuestarias	9
4.2.	Determinación del precio del contrato	11
4.3.	Tramitación del expediente (a efectos presupuestarios)	13
4.4.	Modificación del contrato específico	13
4.5.	Valor estimado	14
4.6.	Contrato financiado con cargo al presupuesto de la Unión Europea	14
5.	LUGAR Y CONDICIONES DE LA ENTREGA	15
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN	15
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	15
7.1.	Ponderación de los criterios de adjudicación	16
7.2.	Fórmula aplicable al criterio precio	16
7.3.	Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio	17
7.3.1.	Criterios evaluables automáticamente mediante fórmulas	17
7.3.2.	Fórmulas para la evaluación automática de los criterios	17
7.4.	Criterios cuya cuantificación depende de un juicio de valor	17
7.4.1.	Criterios y ponderación	17
7.4.2.	Método de valoración y documentación	17
8.	OFERTAS ANORMALMENTE BAJAS	18
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA	18
9.1.	Obligaciones generales	18
9.2.	Otras condiciones de ejecución del contrato	19
9.3.	Obligaciones de seguridad en cumplimiento del ens	19
9.4.	Obligaciones relativas al cumplimiento de las condiciones de los programas ofertados en modalidad de nube cuando exista tratamiento de datos personales	20
10.	PAGO Y FACTURACIÓN	20
10.1.	Pago del precio	20
10.2.	Condiciones de presentación de las facturas	21
11.	GARANTÍA DE LOS BIENES	22



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: 1055154624058134589260

12.	PENALIDADES	22
12.1.	Penalidades fijadas en el sistema dinámico de adquisición	22
12.2.	Fórmula para la aplicación de penalidades	23
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	24
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS	24
	ANEXO I PRESCRIPCIONES TÉCNICAS	27
I.1.	Requisitos funcionales de los programas a suministrar	27
I.2.	Requisitos no funcionales de los programas a suministrar	27
I.3.	Periodo de vigencia y modalidad de licenciamiento	32
I.4.	Requisitos de seguridad de los programas en la nube	33
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO	34
II.1.	Servicios de instalación avanzada de los programas a suministrar	34
II.2.	Servicios de soporte de los programas a suministrar	36
II.2.1.	Dimensionamiento del servicio	36
II.2.2.	Acuerdos de nivel de servicio	36
II.3.	Requisitos de los perfiles profesionales	38
	ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS	38
III.1.	Tratamientos de datos y finalidad de los tratamientos	38
III.2.	Medidas técnicas y organizativas	39
	ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE	40
	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	42
	ANEXO VI Manifestación de conformidad del responsable del tratamiento DE LOS DATOS DEL ORGANISMO	
	DESTINATARIO	44
	ANEXO VII ENTREGAS PARCIALES	45
	ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO	45
	ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN	46
	ANEXO X DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS	
	ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA	47
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	49
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea	49
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR	51



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

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: El mismo

Departamento/organismo: El mismo

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: C/Embajadores 181, 28045 Madrid

Correo electrónico: : licita_agencia_ciber@madrid.org

Teléfono: 91 580 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 DEL LICENCIAMIENTO DE LA PLATAFORMA AUTOMATIZADA DE PRUEBAS DE PENTESTING Y GESTIÓN DE SUPERFICIE DE ATAQUE /INTERNA/EXTERNA EN EL MARCO DEL PRTR, CO-FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU

Objeto del contrato:

El objeto del contrato es el suministro y la ampliación del licenciamiento de una plataforma de pruebas de pentesting y gestión de superficie de ataque externa, a la Comunidad de Madrid por un periodo de 22 meses, actualmente implantada en el organismo, incluyendo los servicios de instalación avanzada y soporte necesarios para ampliar su cobertura funcional y garantizar su correcta operación.

La solución estará dirigida a la validación continua de la postura de seguridad de los sistemas del organismo, permitiendo la ejecución de pruebas de seguridad ofensiva sobre activos internos hasta un máximo de 130.000 endpoints, así como la monitorización y análisis de la superficie de ataque externa asociada a la organización hasta un máximo de 2.500 subdominios, con el objetivo de identificar vulnerabilidades explotables, rutas de ataque potenciales y posibles exposiciones de activos o credenciales en entornos accesibles desde Internet.

El contrato incluirá las actuaciones necesarias para el suministro, la instalación avanzada y la puesta en marcha de la ampliación de licencias de la plataforma, así como el soporte durante el



despliegue y el soporte estándar asociado a la suscripción durante su periodo de vigencia, garantizando su funcionamiento continuo, actualizado y efectivo en los entornos en los que sea implantada.

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:



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

☒ **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 No aplica: categoría Elija una categoría...
- Sistema Haga clic o pulse aquí para escribir texto.: categoría Elija un elemento.
- Haga clic o pulse aquí para escribir texto.

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

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

Relación de los suministros con la arquitectura de seguridad

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

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

Haga clic o pulse aquí para escribir texto.

Aclaración

La plataforma no forma parte directa de la arquitectura de seguridad, al utilizarse como herramienta de validación y evaluación de la postura de seguridad, si bien deberá operar alineada con los principios y requisitos del ENS, garantizando la seguridad y la trazabilidad de la información técnica tratada.

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

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



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

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

- ☒ Los programas objeto del suministro no van a procesar ni almacenar datos de carácter personal, por lo que no existe tratamiento de datos y no son de aplicación ni la Ley Orgánica 3/2018 ni la Ley Orgánica 7/2021. No aplica el apartado 9.4 de este documento de invitación.
- ☐ Los programas objeto del suministro deben procesar o almacenar datos de carácter personal conforme a lo dispuesto en el **Reglamento (UE) 2016/679**, en adelante RGPD, y en la **Ley Orgánica 3/2018**. Se describen las condiciones aplicables en el apartado 9.4 de este documento de invitación.
- ☐ Los programas objeto del suministro deben procesar o almacenar datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, conforme a lo dispuesto en la **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.

Aclaración

El objeto del contrato no requiere tratamiento de datos de carácter personal por parte del adjudicatario, al estar la plataforma orientada exclusivamente a la evaluación técnica de la postura de seguridad de los sistemas del organismo. En caso de analizarse de forma incidental identificadores técnicos asociados a sistemas o cuentas corporativas, dicho análisis se limitará a métricas agregadas y evidencias técnicas, sin explotación de datos personales ni asociación a personas físicas identificadas o identificables. En consecuencia, resulta de aplicación la cláusula de "Protección de datos sin acceso a datos personales", no siendo exigible la condición de encargado del tratamiento conforme al RGPD y la Ley Orgánica 3/2018.

3. DURACIÓN DEL CONTRATO

3.1. FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

- ☒ Al día siguiente al de adjudicación del contrato.
- ☐ El dd/mm/aaaa, salvo que la adjudicación del contrato específico se produzca el mismo día o con posterioridad a dicha fecha, en cuyo caso será la fecha siguiente a la adjudicación del contrato específico.

3.2. PLAZO DE ENTREGA DE LAS LICENCIAS

- ☒ No admite entregas parciales. **Plazo máximo** de entrega³: 15 días naturales contados a partir de la fecha de inicio de ejecución del contrato.

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



☐ Deben realizarse entregas parciales. Los plazos y lugar de las entregas se detallan en el **Anexo VII**.

3.3. PLAZO DE EJECUCIÓN DEL CONTRATO

☐ Se requiere la instalación y configuración básica de las licencias, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo⁴ de 30 días hábiles, incluido el plazo de entrega de las licencias.

☒ El contrato incluye el servicio de instalación avanzada, a prestar por el adjudicatario, descrito en el **Anexo II** apartado 1. El plazo de ejecución de este servicio incluye el plazo para la entrega de las licencias y para la instalación y configuración básica.

- Plazo de ejecución: 30 días hábiles

☒ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario, descritos en el **Anexo II**, apartado 2:

- Plazo de ejecución (señalar únicamente una opción):
 - ☒ 12 meses a contar desde el final de la instalación básica y, en su caso, de la instalación avanzada.
 - ☐ Hasta la expiración de la vigencia de las licencias objeto del suministro.

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

3.4. PRÓRROGA DEL CONTRATO ESPECÍFICO

El presente contrato específico **no es prorrogable**, sin perjuicio de la posibilidad de ampliación del plazo de ejecución descrita en el artículo 29.3 de la LCSP.

4. VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN

4.1. PRESUPUESTO DE LICITACIÓN Y APLICACIONES PRESUPUESTARIAS

Presupuesto total sin impuestos (€)	Impuestos indirectos (€)	Presupuesto total con impuestos (€)
1.500.000,00 €	315.000,00 €	1.815.000,00 €

Detalle del presupuesto de licitación:

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



	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
SUMINISTRO			
Suministro de licencias (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	1.430.915,07 €	300.492,16 €	1.731.407,23 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	55.438,52 €	11.642,09 €	67.080,61 €
Servicio de soporte, a prestar por el adjudicatario	13.646,41 €	2.865,75 €	16.512,16 €
TOTAL	1.500.000,00 €	315.000,00 €	1.815.000,00 €

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

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

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

Aplicación presupuestaria	Anualidad 2026	Anualidad 2027	TOTAL
ACR-015-2026 - SUMINISTRO DEL LICENCIAMIENTO DE LA PLATAFORMA AUTOMATIZADA DE PRUEBAS DE PENTESTING Y GESTIÓN DE SUPERFICIE DE ATAQUE INTERNA/EXTERNA	1.806.743,93 €	8.256,08 €	1.815.000,00 €

El proyecto es cofinanciado con fondos MRR

	Fondos	Anualidad 2026	Anualidad 2027	Total
<i>Fondos MRR</i>	99,09%	1.486.353,59 €		1.486.353,59 €
<i>Fondos Propios</i>	0,91%	6.823,21 €	6.823,21 €	13.646,41 €
IVA		313.567,13 €	1.432,87 €	315.000,00 €
		1.806.743,93 €	8.256,08 €	1.815.000,00 €



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	13.726,08 €
Resto costes directos	1.236.273,92 €
Costes indirectos + Gastos generales + Beneficio industrial	250.000,00 €
Total sin IVA	1.500.000,00 €

Justificación:

El objeto del contrato consiste en la ampliación del licenciamiento de una plataforma de pruebas de pentesting y gestión de superficie de ataque externa, así como en la prestación de los servicios profesionales necesarios para su instalación avanzada, configuración y puesta en funcionamiento.

Además de los costes directos, se han considerado los siguientes conceptos:

Costes indirectos y gastos generales: Calculados como el 14 % de los costes directos, engloban los gastos que no pueden imputarse a una única actividad o recurso, pero que son indispensables para la correcta ejecución del servicio.

Beneficio industrial: Calculado como el 6 % de los costes directos, representa el margen neto razonable de la empresa adjudicataria. Este margen es coherente con los estándares del sector TIC y con la naturaleza especializada de los servicios de ciberseguridad, que requieren inversión constante en tecnología, capacitación y adaptación normativa

En cuanto a los costes directos de personal los importes se calculan tomando como referencia 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 de 16 de abril de 2025, Resolución de 4 de abril de 2025 de la Dirección General de Trabajo), complementado con los ajustes derivados de la especialización tecnológica requerida, los costes sociales y empresariales asociados y los porcentajes de gastos generales y beneficio industrial aplicables a este tipo de servicios:

TABLA DE DESGLOSE DE COSTES DE PERSONAL - SERVICIO DE INSTALACIÓN AVANZADA

A los exclusivos efectos de justificar el presupuesto, y conforme al artículo 100.2 de la Ley 9/2017, se incorpora el desglose estimado de los recursos necesarios para los servicios **de instalación avanzada asociados al suministro**. Esta información tiene carácter estrictamente justificativo y sirve únicamente para motivar el precio, sin exigir adscripción de personal concreto ni implicar una prestación



independiente, manteniéndose la naturaleza de contrato de suministro de software. Los importes y perfiles indicados son una estimación y no generan obligación alguna sobre la organización interna del adjudicatario durante la ejecución del contrato.

Perfiles	Dedicación en horas	Salario Base	Especialización tecnológica (XX%)	Salario anual	Coste anual según dedicación	Cant. Perfiles	Coste personal contrato	Coste personal contrato con Seguridad Social 32%
Gestor/a de Servicio	193	35.674,43	36%	48.517,22 €	5.202,12 €	1	5.202,12 €	6.866,80 €
Responsable técnico	193	35.674,43	36%	48.517,22 €	5.202,12 €	1	5.202,12 €	6.866,80 €
Ing. Automatización (SOAR/Playbooks)	225	35.480,98	20%	42.577,18 €	5.322,15 €	2	10.644,29 €	14.050,4€
Analista de Seguridad	194	35.480,98	23%	43.641,61 €	4.703,60 €	2	9.407,19 €	12.417,49 €
Ingeniero/a de Integración y Despliegue	240	35.480,98	22%	43.286,80 €	5.771,57 €	2	11.543,15 €	15.236,95 €
								55.438,52 €

TABLA DE DESGLOSE DE COSTES DE PERSONAL - EL SERVICIO DE SOPORTE, A PRESTAR POR EL ADJUDICATARIO

Aclaración: El “coste de personal” corresponde a recursos aportados por el proveedor (no plantilla interna) y se utiliza únicamente como base justificativa/dimensionamiento para el precio del servicio de instalación avanzada. No supone una partida adicional independiente en el precio final.

Costes de personal							
Perfiles	Dedicación en horas	Salario Base	Especialización tecnológica (XX%) ⁵	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 32%
Responsable técnico de validación de seguridad	96	35.674,43 €	40%	49.944,20 €	2.663,69 €	2.663,69 €	3.516,07 €
Técnico de despliegue on-premise	147	35.480,98 €	20%	42.577,18 €	3.477,14 €	3.477,14 €	4.589,82 €
Analista de superficie de ataque ext. SaaS	108	35.480,98 €	20%	42.577,18 €	2.554,63 €	2.554,63 €	3.372,11 €
Técnico de remediación y reporting	72	35.480,98 €	20%	42.577,18 €	1.703,09 €	1.703,09 €	2.248,07 €
							13.726,08 €

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

Si bien resulta de aplicación el convenio colectivo sectorial, en el presente servicio se requiere una cualificación superior del personal adscrito, derivada de la experiencia mínima exigida conforme a los criterios de solvencia técnica definidos para cada perfil profesional.

Este mayor nivel de especialización se justifica por el desempeño de funciones de alta complejidad técnica en el ámbito de la ciberseguridad. En consecuencia, el ajuste salarial se realiza mediante la aplicación de una regla proporcional objetiva, consistente en un incremento del **10 % por cada año de experiencia exigido** para los perfiles correspondientes al Área 5 del convenio colectivo de aplicación”

De acuerdo con lo anterior, el ajuste del salario por especialización se aplica del siguiente modo:

- Responsable Técnico del Proyecto: **+40 %** (4 años de experiencia en dirección de proyectos)
- Técnico de despliegue on-premise: **+20 %** (2 años).
- Analista de superficie de ataque ext. SasS: **+20 %** (2 años).
- Técnico de remediación y reporting : **+20 %** (2 años).

Incremento por cotizaciones y cargas sociales (32 %)

Se incorpora el coste correspondiente a las cotizaciones empresariales a la Seguridad Social, calculado como el **32 % del salario ajustado**, conforme a los porcentajes habituales aplicables a este tipo de perfiles.

Otros costes directos del profesional (6 %)

Este porcentaje recoge los costes directos complementarios imputables al personal adscrito al servicio, incluyendo, entre otros:

- Material y equipamiento informático.
- Suscripciones o licencias de software necesarias para el desempeño de las funciones.
- Seguro de responsabilidad civil profesional y de accidentes.
- Gastos de comunicación y conectividad asociados a los medios de trabajo...

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:

NO APLICA

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

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

4.5. VALOR ESTIMADO

Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **UN MILLÓN QUINIENTOS MIL. euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	1.500.000,00 €
Importe máximo por modificación prevista, sin IVA	0.00 €
TOTAL	1.500.000,00 €

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: SI01 (submedida de inversión 01)/NextGenerationEU (Fondo de Recuperación) /Programa PRTR/ Mecanismo de Recuperación y Resiliencia (MRR)

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

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

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



obligado cumplimiento al presente contrato las obligaciones establecidas en la Adenda para contratos cofinanciados con cargo al presupuesto de la Unión Europea.

5. LUGAR Y CONDICIONES DE LA ENTREGA

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

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

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

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

6. INCOMPATIBILIDADES PARA LA LICITACIÓN

☒ **No ha existido participación de empresas** en la elaboración de las especificaciones técnicas o los documentos preparatorios del contrato específico, ni existen incompatibilidades por causas de la naturaleza de los trabajos a realizar por el adjudicatario.

☐ **Sí han participado empresas** en la elaboración de especificaciones técnicas o de los documentos preparatorios del contrato específico. Se han adoptado las siguientes medidas para garantizar que su participación en la licitación no falsee la competencia:

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

☐ Otras:
(*Detallar en su caso*)

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

7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN⁷

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



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
No aplica	No aplica

- ☐ 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
No aplica	No aplica	No aplica

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**:

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

Donde:

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

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

Función **Minimizar**:

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

Donde:

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

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

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

$$X_i = P$$

Donde:

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

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

No aplica

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*.

Alternativamente, se podrá sustituir la anterior regla general por una regla particular conforme al artículo 149 de la LCSP. La inclusión de una regla particular requerirá que ésta haya sido previamente validada por el Servicio Jurídico del organismo destinatario.

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:

No aplica

- 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 aplica

9.3. OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

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

En cumplimiento del artículo 13.5 del ENS, es obligación del adjudicatario designar una Persona de Contacto (POC) que canalice y supervise el cumplimiento de los requisitos de seguridad exigidos en esta cláusula y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes de seguridad durante la ejecución del contrato específico. Dicha Persona de Contacto será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

En caso de que el contrato específico incluya la prestación de servicios por parte del adjudicatario, el organismo destinatario informará de sus deberes, obligaciones y responsabilidades en materia de seguridad en lo relativo al sistema de información al personal puesto a disposición para la prestación del citado servicio, en cumplimiento del artículo 15 del ENS. Esta información se realizará en la fase de ejecución del contrato. Es obligación del adjudicatario supervisar la actuación de dicho personal, para verificar que se siguen los procedimientos establecidos por el organismo, se aplican las normas indicadas y los procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.



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

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

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

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

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

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

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

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

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



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

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

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

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

10.2. CONDICIONES DE PRESENTACIÓN DE LAS FACTURAS

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

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): A13037574
- Órgano gestor (DIR3): A13037574
- Unidad tramitadora (DIR3): A13037574
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3): A13037574

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 para la Administración Digital de la Comunidad de Madrid gestionará, con un procedimiento automatizado, las facturas recibidas en el "Punto General de Entrada de Facturas Electrónicas", FACe, en los términos establecidos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y sus disposiciones de desarrollo.



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

- Órgano de contratación: Agencia para la Administración Digital de la Comunidad de Madrid - Q7850054C.
- Código DIR3: El código único para el órgano gestor, la unidad tramitadora y la oficina contable es el A13037574.

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

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	No aplica	Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo	No aplica	N/A



Incumplimiento de los compromisos de adscripción de medios.	2% de la facturación del periodo	No aplica	Apartado 12.2
Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas.	2% de la facturación del periodo	No aplica	Apartado 12.2
Demora en el cumplimiento del plazo total del contrato	Resolución / 0,60 euros por cada día y 1.000 euros del precio del contrato, IVA excluido		Valor fijado en el SDA
Incumplimiento de obligaciones en materia medioambiental, social o laboral	2% de la facturación del periodo		Apartado 12.2
Incumplimiento de las condiciones de subcontratación	2% del importe del subcontrato		Valor fijado en el SDA
Incumplimiento de las obligaciones de información y pago sobre suministradores y subcontratistas.	2% del importe del subcontrato		Valor fijado en el SDA

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

- El incumplimiento de las medidas relativas a la seguridad de los programas en cumplimiento del ENS, o de los requisitos de seguridad para la protección de datos personales en nube tendrá la consideración de incumplimiento **muy grave** dando lugar a una penalidad de hasta el **10% del importe total del contrato**.
- Incumplimiento del resto de las condiciones especiales de ejecución
 - Grave: N/A
 - Muy grave: N/A
- Incumplimiento de los ANS:
 - Grave: N/A
 - Muy grave: N/A
- Incumplimiento de los compromisos de adscripción de medios
 - Grave: N/A
 - Muy grave: N/A
- Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas
 - Grave: N/A
 - Muy grave: N/A

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:



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

- 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 PLACSP⁹ u otra plataforma de contratación a disposición del organismo.

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

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

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

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 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:
 - *Fichas técnicas de los productos detallados en la oferta, si corresponde.*
 - *Documento justificativo en el que se detalle mediante una matriz de cumplimiento los requisitos funcionales de la solución.*

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

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



○ *Certificación de ENS de la solución a ofertar.*

- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - N/A
- 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.

- Haga clic o pulse aquí para escribir texto.

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

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

Para consultas se habilita un plazo de 3 días naturales a contar desde el día siguiente de la recepción de la invitación a participar en la licitación.

Las consultas se remitirán por correo electrónico a la siguiente dirección de correo electrónico:

licita_agencia_ciber@madrid.org

Con la finalidad de dar cumplimiento a las medidas destinadas a las entidades adheridas para velar por la correcta aplicación de los términos, condiciones e instrucciones que regulan el Sistema Dinámico de Adquisición de suministro de software de sistema, de desarrollo y de aplicación (SDA 25/2022), los pliegos rectores del SDA se encuentran disponibles en el siguiente enlace:

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): Consejero Delegado de la Agencia de
Ciberseguridad de la Comunidad de Madrid

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

Firmado digitalmente por: LAS HERAS VÁZQUEZ ALEJANDRO
Fecha: 2026.03.20 12:36



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

ANEXO I PRESCRIPCIÓN TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

La Agencia para la Administración Digital de la Comunidad de Madrid requiere la ampliación del licenciamiento y la instalación avanzada de una plataforma de pruebas de pentesting y gestión de superficie de ataque externa, con el fin de reforzar la postura de seguridad de la entidad frente a amenazas cibernéticas.

El presente contrato tiene por objeto **extender las capacidades de la solución actualmente en uso por el organismo**, ampliando el alcance de la validación de seguridad sobre activos internos hasta **130.000 endpoints** y las capacidades de gestión y monitorización de la superficie de ataque externa hasta **2.500 subdominios**, de acuerdo con las nuevas necesidades funcionales del servicio.

La ampliación se realizará sobre la solución existente, **sin modificación estructural de la arquitectura actualmente desplegada y garantizando la compatibilidad con la configuración operativa implantada**.

La solución deberá permitir evaluar de forma continua y sistemática la efectividad de los controles de seguridad existentes, mediante la ejecución de pruebas de seguridad ofensiva controladas sobre los sistemas del organismo y la monitorización de la superficie de ataque externa asociada a la organización.

La plataforma deberá permitir la evaluación continua de la eficacia de los controles de seguridad del organismo, mediante la identificación, análisis, validación y priorización de vulnerabilidades explotables, rutas de ataque potenciales y exposiciones de seguridad sobre la infraestructura tecnológica, tanto en activos internos como en la superficie de ataque externa asociada a la organización. La solución deberá proporcionar una gestión centralizada a través de una única consola, sin necesidad de agentes en los sistemas objeto de validación interna ni de despliegues complejos, facilitando la supervisión integrada de resultados, la priorización de las acciones de remediación y la mejora de la capacidad de detección y respuesta ante amenazas.

El modelo de licenciamiento deberá garantizar el derecho de uso de la solución por un periodo de **22 meses**, asegurando acceso a actualizaciones, soporte técnico y mejoras de funcionalidad durante toda la vigencia del contrato.

Las características principales que se pretenden obtener con el despliegue de esta solución son:

- **Pruebas de pentesting sobre activos internos**, mediante técnicas equivalentes a las empleadas por actores reales.
- **Validación de explotación real**, permitiendo determinar qué vulnerabilidades, configuraciones inseguras o rutas de ataque resultan efectivamente explotables en el entorno evaluado.
- **Evaluación continua de la postura de seguridad**, mediante la ejecución recurrente de ejercicios de validación.
- **La solución deberá permitir la validación interna sin necesidad de agentes** (evitando la instalación de componentes adicionales en los sistemas objeto de evaluación) **en el caso general; en caso de requerirse componentes puntuales, deberán ser de despliegue mínimo, controlado y plenamente justificado, sin impacto operativo.**



- **Priorización de hallazgos en función del riesgo efectivo**, atendiendo a la explotabilidad real y al impacto potencial sobre los activos del organismo.
- **Gestión de superficie de ataque externa**, permitiendo la identificación, monitorización y análisis de activos expuestos en Internet asociados a la organización.
- **Compatibilidad con las soluciones de seguridad existentes**, permitiendo su utilización en entornos con herramientas de detección, monitorización y respuesta ya implantadas.
- **Gestión centralizada**, mediante una consola unificada para la consulta integrada de resultados, hallazgos y recomendaciones de remediación.

La solución deberá cumplir con estándares y mejores prácticas de seguridad internacionalmente reconocidos, garantizando su alineación con marcos normativos y metodologías de referencia en ciberseguridad. En este sentido, la plataforma deberá permitir la validación de controles de seguridad utilizando tácticas, técnicas y procedimientos alineados con el marco **MITRE ATT&CK**, facilitando la identificación y mitigación de amenazas reales. Asimismo, su metodología deberá estar alineada con las recomendaciones del **NIST** para la evaluación continua de la exposición a amenazas y contribuir al cumplimiento del **Esquema Nacional de Seguridad (ENS)**, reforzando la protección de los activos críticos de la entidad.

El razonamiento expuesto justifica la necesidad de especificar una plataforma de **pruebas de pentesting y gestión de superficie de ataque externa** en los términos descritos, sin que ello implique una vulneración del principio de neutralidad tecnológica, conforme al artículo 126 de la Ley de Contratos del Sector Público. No se pretende, por tanto, restringir la competencia, sino garantizar la adecuación de la solución a los requisitos técnicos y operativos de la Agencia de Ciberseguridad de la Comunidad de Madrid. La equivalencia deberá entenderse en los términos que define el apartado III.1 del Pliego de Prescripciones Técnicas.

Se detallan a continuación las características indispensables de la solución, siendo obligatorio el cumplimiento de todos los puntos que se detallan a continuación:

Requisitos funcionales del programa

REQ 1. Capacidades de validación interna y explotación controlada

La solución deberá permitir la ejecución de pruebas automatizadas de validación de seguridad mediante técnicas equivalentes a las empleadas por actores reales, garantizando un entorno de ejecución controlado, auditado y reversible.

REQ 1.1. Pentesting automatizado sin agentes

La plataforma deberá ejecutar pruebas de seguridad sin necesidad de instalar agentes en los sistemas objetivo, evitando impacto operativo, modificaciones estructurales o dependencias adicionales.

REQ 1.2. Explotación ética real

La solución no deberá limitarse a la identificación teórica de vulnerabilidades, sino que deberá realizar explotación ética real y controlada para determinar:

- Explotabilidad efectiva en el contexto del organismo.
- Nivel de acceso alcanzable.
- Impacto potencial sobre activos críticos.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

Todas las acciones deberán ejecutarse de forma segura, sin alteración permanente de los sistemas.

REQ 1.3. Validación de rutas completas de ataque

La plataforma deberá permitir identificar y validar cadenas completas de ataque (Attack Path Validation), incluyendo, entre otras:

- Encadenamiento de vulnerabilidades, es decir, utilización de varios CVEs o errores de configuración para un mismo vector de ataque.
- Movimiento lateral, utilizando los protocolos y métodos más comunes por los actores maliciosos.
- Escalado de privilegios. La solución valida si es posible obtener privilegios administrativos mediante la explotación controlada de vulnerabilidades o configuraciones inseguras.
- Acceso a activos críticos. La plataforma verifica si, desde un punto inicial de compromiso, pueden alcanzarse activos críticos mediante el encadenamiento de técnicas de ataque.
- Extracción y validación controlada de credenciales.

Este enfoque permite priorizar la remediación en función del riesgo real.

REQ 1.4. Técnicas incorporadas

Las técnicas incorporadas deberán mapearse con el marco MITRE ATT&CK desde las fases iniciales de acceso y reconocimiento hasta las fases finales de impacto y exfiltración, permitiendo una trazabilidad completa del ciclo de ataque.

REQ 1.5. Validación de Active Directory

La ampliación deberá mantener y extender las capacidades de evaluación sobre entornos Active Directory, permitiendo:

- Identificación de contraseñas débiles.
- Detección de cuentas con contraseñas que no expiran.
- Identificación de grupos con privilegios excesivos.
- Comparación de credenciales internas frente a credenciales expuestas públicamente, incluyendo coincidencias exactas y variantes derivadas.

Las verificaciones sobre entornos de Active Directory se realizarán exclusivamente a efectos de evaluación técnica de la postura de seguridad, sobre objetos y cuentas corporativas, sin incorporación de datos personales adicionales. Los resultados de la validación se limitarán a métricas agregadas, evidencias técnicas y hallazgos de seguridad, sin tratamiento de datos personales, conforme a lo indicado en el apartado de protección de datos del Documento de Invitación.

REQ 1.6. Validación de vulnerabilidades explotables

La solución deberá validar vulnerabilidades realmente explotables en el entorno evaluado, incluyendo aquellas recogidas en el catálogo CISA KEV (Known Exploited Vulnerabilities).

Los hallazgos deberán priorizarse conforme a su explotabilidad efectiva y su impacto real en el contexto del organismo.



REQ 1.7. Emulación controlada de campañas de ransomware

La plataforma deberá permitir ejecutar campañas controladas que incluyan:

- Emulación de cifrado. La solución deberá crear una copia de los ficheros para posteriormente cifrarlos. De esta forma se deberá conseguir evaluar el EDR sin llegar a provocar ningún impacto en los activos donde se lance.
- Emulación de exfiltración. Deberá permitir comprobar si las herramientas de protección detectan y bloquean conexiones de Command and Control (C2) como parte del ataque de ransomware.
- Técnicas avanzadas de compromiso y movimiento lateral para evaluar la configuración y las capacidades de detección y bloqueo del EDR. Se deberán incluir técnicas de bypass y ofuscación, así como acciones controladas típicas de este tipo de ataques como el intento de deshabilitar el EDR.

Estas acciones deberán realizarse sin afectar a la operativa productiva.

REQ 1.8. Integración y validación del SOC

La solución deberá permitir la integración con herramientas SIEM existentes, facilitando la validación de la capacidad de detección y respuesta del SOC.

Asimismo, deberá permitir:

- Generación de alertas ante explotaciones exitosas.
- Auditoría de eventos generados.
- Trazabilidad completa de los ejercicios ejecutados.

REQ 2. Gestión de Superficie de Ataque Externa

La ampliación contempla capacidades de gestión de superficie de ataque externa que incluyen:

- Gestión de hasta 2.500 subdominios externos asociados a uno/varios dominios externos.
- Descubrimiento automático de activos externos asociados a los dominios proporcionados al fabricante.
- Escaneo automático semanal de dichos dominios principales facilitados al inicio en busca de nuevos activos expuestos como pueden ser IPs, webs, servicios, etc
- Validaciones de explotación diarias, permitiendo el lanzamiento de acciones controladas manuales sobre ciertos activos con el objetivo de retestear una vulnerabilidad, comprobar si un vector de ataque es exitoso, si una credencial expuesta es válida, entre otros.
- Identificación de elementos como:
 - Servicios expuestos involuntariamente.
 - Errores de configuración.
 - Puertos abiertos.
 - Certificados inseguros.
 - Servicios obsoletos.
 - Vulnerabilidades explotables.
 - Credenciales expuestas.

La solución deberá permitir:



- Priorización basada en explotabilidad real segura.
- Visibilidad de cadenas completas de ataque.
- Histórico de exposición, indicando cuando días el activo fue vulnerable.
- Generación de informes técnicos y ejecutivos. Además, se deberán poder incluir tags en los diferentes activos (dominios, subdominios, IPs, webs, etc) y obtener un informe en base a los mismos.
- Validación controlada de credenciales expuestas **asociadas a activos corporativos**, mediante intentos limitados para evitar bloqueos; **sin tratamiento de datos personales** y conforme al marco indicado en el apartado de protección de datos del DI.

REQ 3. Arquitectura y modalidad de operación

La plataforma estará compuesta de dos componentes con alcances para ejercer las funciones en ámbitos diferentes.

REQ3.1 componente de validación interna

Funcionalidades obligatorias:

- Reconocimiento autónomo continuo de red interna
- Identificación automatizada de vulnerabilidades, configuraciones débiles y brechas de higiene
- Ejecución de exploits seguros contra endpoints para validar controles reales
- Simulación de TTPs de atacantes (MITRE ATT&CK) en entornos internos
- Verificación específica de defensas anti-ransomware
- Priorización por causas raíz con guías de remediación precisas

Arquitectura: Despliegue local, Conectividad saliente mínima (actualizaciones), |
Reutilización hardware existente

REQ3.2, Componente de Validación Externa (SaaS puro)

Funcionalidades obligatorias:

- Mapeo continuo de activos expuestos (OSINT + reconocimiento activo)
- Validación de vulnerabilidades explotables en aplicaciones web (OWASP Top 10)
- Detección de credenciales filtradas vía credential stuffing
- Identificación de vectores externos atractivos para adversarios
- Alertas de nuevas exposiciones perimetrales en tiempo real

Arquitectura: 100% SaaS, Sin instalación, Acceso web/API, Dominios específicos para escaneo inicial

REQ 3.3. Integración y escalabilidad

- Solución única que integre ambos componentes con consola unificada
- Ampliaciones sin cambios estructurales en arquitectura existente
- Memoria técnica obligatoria: Diagramas arquitectura híbrida, flujos datos, justificación ENS/Zero-Trust

Se deberá justificar el cumplimiento exacto de capacidades funcionales diferenciadas por componente arquitectónico.

El componente de validación interna podrá requerir conectividad saliente mínima exclusivamente para fines de actualización, mantenimiento y soporte del producto, hacia los dominios que el fabricante identifique y documente. Dicha conectividad no



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

implicará transferencia de datos internos distintos de los estrictamente necesarios para la operación técnica de la solución, conforme a las políticas de seguridad del organismo.

REQ 4. Soporte por parte del fabricante

El servicio de soporte deberá prestarse conforme al Acuerdo de Nivel de Servicio (SLA) del fabricante (documento adjunto) incluyendo actualizaciones, parches y asistencia técnica remota durante horario laboral, con tiempos de respuesta definidos según la criticidad de la incidencia (desde 6 horas laborables para incidencias críticas hasta 5 días laborables para incidencias menores). El modelo deberá contemplar escalado técnico multinivel hasta soporte de producto y equipo técnico especializado, garantizando trazabilidad, gestión formal de tickets y resolución conforme a la severidad del caso.

REQ 5. Instalación y puesta en marcha

Componente de validación interna (on-premise):

- Se deberá reutilizar el hardware empleado en la fase inicial, sin necesidad de reposición.
- Para la presente ampliación, el licitador/fabricante analizará la arquitectura de red existente y, en su caso, aconsejará la incorporación de nodos o elementos adicionales mínimos, con el objetivo de maximizar las capacidades de la plataforma y su gestión.
- Las propuestas de ampliación deberán priorizar la menor modificación posible de la infraestructura y de las reglas de seguridad, garantizando la continuidad operativa.
- Una vez adjudicado el contrato, se deberá aportar un documento técnico que amplíe la información relativa a la instalación, arquitectura y primeros pasos de la solución (guía de instalación).

Componente de validación externa (SaaS):

- Modalidad 100 % SaaS, sin requerir instalación ni infraestructura local.
- Identificación de los dominios y/o endpoints específicos necesarios para la configuración inicial y los escaneos, que deberán detallarse en la memoria técnica presentada por el licitador.

Escalabilidad general:

- Compatibilidad total con la arquitectura preexistente, garantizando la continuidad operativa y una mínima intervención técnica.

REQ 6. Seguridad y cumplimiento normativo

La solución:

- Deberá garantizar integridad y confidencialidad de la información tratada.
- Deberá operar sin transferencia de datos internos fuera del entorno del organismo.
- Deberá permitir auditoría completa de acciones realizadas.
- Deberá mantener trazabilidad integral de ejercicios ejecutados.
- Deberá adecuarse a los requisitos del Esquema Nacional de Seguridad (ENS), conforme a la categoría aplicable.

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

N/A

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO



Vigencia de las licencias:

Part Number	Programa	Periodo de vigencia del licenciamiento
Pentera Core Plus Enterprise - 130,000 End Points o equivalente	Plataforma de pruebas de pentesting sobre activos internos, en modalidad on-premise, incluyendo capacidades de validación interna y explotación controlada, validación de rutas completas de ataque, validación de Active Directory, validación de vulnerabilidades explotables, emulación controlada de campañas de ransomware e integración y validación del SOC, o solución equivalente.	22 Meses
Pentera Surface Prime - 2,500 Subdomains o equivalente	Plataforma de gestión de superficie de ataque externa, en modalidad SaaS, incluyendo descubrimiento automático de activos externos, monitorización de dominios y subdominios, validación de exposición y generación de informes técnicos y ejecutivos, o solución equivalente.	22 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
Pentera Core Plus Enterprise o equivalente - 130,000 End Points	<ul style="list-style-type: none"> Derecho de uso: durante la vigencia de la suscripción, conforme al alcance licenciado para validación de seguridad sobre activos internos y gestión de superficie de ataque externa. Derecho de actualización: acceso a actualizaciones, parches y versiones disponibles durante la vigencia de la suscripción, conforme al modelo de mantenimiento y soporte del fabricante. Derecho de acceso a documentación: acceso a la documentación técnica y manuales del fabricante. Derecho de consulta al fabricante: <ul style="list-style-type: none"> Horario: 8x5 Tiempo de respuesta: en función de la criticidad de la incidencia, desde 6 horas laborables para incidencias críticas hasta 5 días laborables para incidencias menores.
Pentera Surface Prime - o equivalente - 2,500 Subdomains	

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



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

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

Alcance

Los servicios de instalación avanzada se aplicarán a los programas objeto del suministro y deberán incluir las actuaciones necesarias para garantizar la correcta implantación, configuración inicial y puesta en funcionamiento de la ampliación de la plataforma de pruebas de pentesting y gestión de superficie de ataque externa en el entorno tecnológico del organismo.

La instalación avanzada se realizará sobre la solución actualmente en uso por el organismo, garantizando la continuidad de la arquitectura existente y la compatibilidad con la configuración ya implantada.

En particular:

- La **plataforma de validación de seguridad interna** deberá desplegarse en infraestructura del organismo en modalidad on-premise, conforme a los requisitos técnicos definidos por el fabricante.
- La **plataforma de gestión de superficie de ataque externa** opera en modalidad SaaS, por lo que no requiere instalación en la infraestructura del organismo, siendo

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



únicamente necesaria su configuración inicial para el inicio de la monitorización de dominios.

Los servicios de instalación avanzada tendrán como objetivo asegurar que la solución quede **operativa, correctamente configurada y alineada con el entorno tecnológico del organismo.**

SERVICIOS INCLUIDOS EN LA INSTALACIÓN AVANZADA

Para la instalación de la plataforma de validación interna, el organismo proporcionará la infraestructura necesaria conforme a los requisitos técnicos definidos por el fabricante.

Como parte de la instalación avanzada, el adjudicatario deberá realizar, como mínimo, las siguientes actividades:

- **Revisión del entorno técnico y planificación de despliegue**
Análisis del entorno tecnológico del organismo para verificar la adecuación de la infraestructura disponible y la conectividad necesaria para el despliegue de la solución.
- **Despliegue e instalación**
Despliegue del nodo principal de la solución en la infraestructura definida por el organismo, incluyendo la instalación del software necesario conforme a los requisitos del fabricante.
- **Configuración inicial de la plataforma**
Configuración de los parámetros iniciales de operación, incluyendo interfaces de red, conectividad, acceso administrativo y parámetros básicos de funcionamiento.
- **Configuración de la superficie de ataque externa**
Configuración inicial de los dominios y subdominios que serán objeto de monitorización en la plataforma de gestión de superficie de ataque externa, así como activación de los parámetros básicos necesarios para el inicio del servicio.
- **Optimización y personalización de la plataforma**
Ajuste de la configuración inicial de la solución a las características del entorno del organismo, con el fin de facilitar su operación, cobertura funcional y adecuación a la arquitectura existente.
- **Validación y pruebas de funcionamiento**
Realización de pruebas iniciales de funcionamiento para comprobar la correcta operación de la solución, la conectividad entre componentes y la generación de resultados conforme a las funcionalidades previstas.
- **Documentación y entrega de manual de operación**
Entrega de la documentación técnica necesaria para la operación de la solución, incluyendo referencias a la documentación oficial del fabricante y de la configuración realizada.
- **Asistencia técnica por parte del fabricante.**
Durante la instalación avanzada se deberá disponer de la asistencia técnica por parte del fabricante de la solución ofertada, para la correcta implantación, configuración y validación de la solución.

PLAN DE IMPLANTACIÓN

El adjudicatario deberá presentar un Plan de Implantación que describa la metodología prevista para la ejecución de los trabajos necesarios para la instalación avanzada.

Este plan deberá contemplar, como mínimo, las siguientes fases:

- **Fase de inicio**



Incluye la planificación inicial del proyecto y la coordinación con el organismo para la validación del alcance de los trabajos, la definición de los entornos de despliegue y la revisión de los requisitos técnicos necesarios para la instalación.

- **Fase de instalación y configuración**

Incluye el despliegue de la plataforma en la infraestructura definida por el organismo y la configuración inicial de los parámetros necesarios para su funcionamiento.

- **Fase de validación**

Incluye la verificación del funcionamiento de la solución tras su instalación, mediante la ejecución de pruebas iniciales que permitan comprobar la correcta operación de las funcionalidades principales.

- **Fase de cierre**

Incluye la entrega de la documentación asociada a la instalación y la confirmación de la correcta puesta en funcionamiento de la solución.

La finalización de los trabajos de instalación avanzada estará sujeta a la validación por parte del responsable designado por el organismo.

La plataforma de gestión de superficie de ataque externa no requiere despliegue de infraestructura en el entorno del organismo, siendo únicamente necesaria la configuración de los dominios que serán objeto de monitorización.

El adjudicatario deberá proporcionar el personal cualificado para la ejecución de todos los trabajos requeridos y deberá designar un jefe de proyecto dedicado para la Comunidad de Madrid, que actuará como interlocutor directo con el Responsable del Proyecto designado por la Agencia.

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

Alcance:

El adjudicatario prestará el servicio de soporte asociado al suministro del licenciamiento de la plataforma de pentesting, con el objeto de garantizar la correcta operación, disponibilidad y mantenimiento ordinario de la solución durante la vigencia del contrato.

Dicho soporte comprenderá las actuaciones necesarias para asegurar que la plataforma suministrada se mantenga correctamente configurada, integrada y operativa, conforme a los requisitos técnicos, de seguridad y de cumplimiento normativo aplicables, y dentro de los parámetros y configuraciones establecidos en la solución licenciada.

El adjudicatario asumirá la responsabilidad sobre la adecuada prestación del soporte asociado al licenciamiento, sin que ello implique la realización de desarrollos, modificaciones funcionales o alteraciones de la arquitectura de la solución más allá de las previstas en el alcance del suministro y del soporte contratados.

II.3. DIMENSIONAMIENTO DEL SERVICIO

Las incidencias se catalogarán de acuerdo a los siguientes niveles de severidad, según su impacto en la operatividad de la plataforma:

- **Incidencias críticas:** afectan la disponibilidad o funcionalidad central de la plataforma.
 - Fallo total en la plataforma.



- Interrupción en la ejecución de pruebas de pentesting.
- Pérdida de acceso a la plataforma.
- Fallo en la actualización de software.
- Interrupción de funcionalidades esenciales de validación de seguridad sin alternativa de continuidad.
- **Incidencias Graves:** afectan funcionalidades específicas sin comprometer la operatividad general.
 - Errores en la detección de vulnerabilidades.
 - Inconsistencia en los informes.
 - Problemas de conectividad con ciertos activos o segmentos de red.
 - Afectación significativa a una parte relevante de la operativa del producto, sin impedir completamente la continuidad del servicio.
- **Incidencias medias o leves:** consultas, ajustes menores o solicitudes de optimización.
 - Consultas sobre configuración.
 - Ajustes en la programación de pruebas de pentesting.
 - Modificación de credenciales de acceso para pruebas avanzadas.
 - Soporte en la interpretación de reportes.
 - Errores menores en la visualización de datos o interfaz.

II.3.1. ACUERDOS DE NIVEL DE SERVICIO

A efectos de cálculo del cumplimiento de los ANS, sólo computa el tiempo transcurrido dentro del horario de prestación del servicio descrito en el apartado anterior y atendiendo al dimensionamiento anterior. 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.

En base a estos niveles de prioridad, el licitador garantizará unos niveles de servicio que comprenden el horario de servicio y los tiempos máximos de respuesta y de resolución, que se recogen en la siguiente tabla:

Id.	Nombre	Descripción del indicador	Valor
ANS_01	Tiempo de respuesta de incidencia leve	Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha comenzado a trabajar en su resolución.	5 días laborables en 8x5
ANS_02	Tiempo de resolución de incidencia leve	Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha comenzado a trabajar en su resolución.	5 días laborables en 8x5
ANS_03	Tiempo de resolución de incidencia media	Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha comenzado a trabajar en su resolución.	2 días laborables
ANS_04	Tiempo de resolución de incidencia grave		1 día laborable siguiente en 8x5
ANS_05	Tiempo de resolución de incidencia crítica		5 horas en 8x5
...



Nota. - Los cálculos de horas, se entienden en horas naturales dentro del horario de servicio indicado. Se tomará como momento de notificación la fecha y hora: minutos en la que el personal de la Comunidad de Madrid realiza la notificación por medio correo electrónico o atención telefónica o una herramienta web de gestión de incidencias.

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.4. REQUISITOS DE LOS PERFILES PROFESIONALES

Para la correcta ejecución del contrato no se establecen requisitos de adscripción individual (titulación, experiencia o certificaciones) para los profesionales asignados por el adjudicatario.

La prestación del contrato se centra en el suministro de licencias de software y en los servicios complementarios de instalación avanzada asociados al producto, de acuerdo con las especificaciones técnicas y los acuerdos de nivel de servicio establecidos.

En consecuencia:

- No se exige la identificación previa del personal adscrito ni la aportación de certificaciones individuales específicas como requisito de licitación.
- La responsabilidad sobre la dotación adecuada de personal técnico y operativo corresponderá al adjudicatario, quien deberá garantizar la correcta ejecución de las tareas comprometidas y el cumplimiento de los niveles de servicio y seguridad definidos en el contrato.
- El cumplimiento de los requisitos se verificará sobre la prestación efectiva del servicio y el correcto funcionamiento de la plataforma, sin perjuicio de que el adjudicatario deba asegurar la cualificación adecuada de los recursos asignados.

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: Haga clic o pulse aquí para escribir texto.
- Categorías de datos personales tratados: Haga clic o pulse aquí para escribir texto.
- Datos sensibles tratados (si procede) y restricciones o garantías aplicables: Haga clic o pulse aquí para escribir texto.



- Naturaleza del tratamiento: Haga clic o pulse aquí para escribir texto.
- Finalidad(es) del tratamiento: Haga clic o pulse aquí para escribir texto.
- Duración del tratamiento: Haga clic o pulse aquí para escribir texto.

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:

En este apartado deberá indicar las medidas concretas necesarias.

ADVERTENCIA: *En todo caso, se recuerda que los tratamientos y medidas técnicas u organizativas deben establecerse conforme al análisis de riesgos y que en los supuestos en los que se demandan soluciones concretas deberían comprobarse las que incorporan los proveedores de nube en los que se van a utilizar los suministros que se contratan.*



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

Contratos previos asociados con la instalación existente:

Contrato	Fecha adjudicación	Importe	Objeto
ACR-006-2026	20-01-2026	214.125,32 €	El objeto del contrato consiste en el suministro y puesta en explotación de una plataforma de validación automatizada de seguridad, incluyendo el licenciamiento inicial con un alcance de hasta 9.000 endpoints, así como los servicios de operación y configuración necesarios para su correcta implantación, la generación de informes de resultados y la definición de modelos de escenarios de validación, conforme a las necesidades operativas del organismo.

La Agencia de Ciberseguridad de la Comunidad de Madrid dispone actualmente de una solución tecnológica de validación automatizada de seguridad y pruebas de penetración automatizadas, implantada y en explotación, basada en Pentera, adquirida en el marco del expediente ACR-006-2026, que incluye el uso de Pentera Core Plus Enterprise con una cobertura inicial de 9.000 endpoints, así como funcionalidades de simulación controlada, reporting y priorización de vulnerabilidades explotables.

Dicha solución se encuentra integrada en el entorno tecnológico de la Agencia y da soporte a procesos de validación continua de controles de seguridad, identificación de vulnerabilidades explotables, análisis de rutas de ataque y seguimiento de la exposición a amenazas, ajustados a las necesidades operativas de la organización.

El objeto del presente contrato específico (ACR-015-2026) consiste en el suministro y ampliación del licenciamiento de la plataforma de pentesting ya implantada, incorporando y/o ampliando las capacidades de gestión de superficie de ataque externa, incrementando su cobertura funcional y escalando el alcance de validación sobre activos internos hasta 130.000 endpoints y la monitorización de la exposición externa hasta 2.500 subdominios, manteniendo la continuidad tecnológica y operativa durante un periodo de 22 meses.

La compatibilidad con la instalación existente resulta técnicamente necesaria para garantizar:

- La continuidad del servicio y la reutilización de las configuraciones ya implantadas, incluyendo escenarios de validación, políticas de intrusividad y contención, criterios de priorización y modelos de reporting.
- La comparabilidad temporal de los resultados técnicos, tales como vulnerabilidades explotables, rutas de ataque verificadas, evolución de la exposición y trazabilidad de las acciones de remediación.
- La minimización de riesgos técnicos y organizativos derivados de una eventual sustitución tecnológica, que implicaría reconfiguraciones completas del entorno, recalibración de escenarios y reconstrucción de evidencias históricas.

La implantación de una solución tecnológicamente diferente supondría, necesariamente, la modificación sustancial de los modelos de simulación y segmentación existentes, la realización de nuevas validaciones funcionales para garantizar la equivalencia de resultados, la asunción de un riesgo técnico y organizativo adicional asociado a la transición entre plataformas, así como un impacto negativo en los plazos de puesta en servicio y en la continuidad de las series históricas de datos.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

Desde el punto de vista de la eficiencia en la gestión de los recursos públicos, la compatibilidad con la solución actualmente implantada permite aprovechar las configuraciones y parametrizaciones ya desarrolladas, evitar duplicidades de costes técnicos y económicos, garantizar la continuidad de los procesos de medición y seguimiento del riesgo de seguridad, y reducir el impacto organizativo derivado de la implantación de una nueva solución.

Asimismo, el presente contrato específico incorpora como ampliación funcional nuevas capacidades de gestión y monitorización de la superficie de ataque externa, integradas en la misma plataforma tecnológica que soporta el componente de validación interna ya implantado. Esta ampliación permite extender el alcance de la validación de seguridad hacia activos expuestos en Internet, manteniendo una consola unificada, modelos de análisis homogéneos y criterios comunes de priorización del riesgo, sin introducir soluciones tecnológicas adicionales ni rupturas en la arquitectura existente.

La incorporación de dichas capacidades externas se concibe, por tanto, como una extensión natural y coherente de la solución actualmente en uso, garantizando la continuidad operativa, la trazabilidad de resultados y la eficiencia en la gestión de los recursos públicos.

En consecuencia, y exclusivamente a efectos de garantizar la referida compatibilidad técnica, el Documento de Invitación podrá hacer referencia a la solución actualmente implantada del fabricante Pentera, o en su caso, a soluciones funcionalmente equivalentes.

La referencia a un producto concreto se realiza de forma justificada y proporcionada, al amparo de lo previsto en la normativa de contratación pública, y no tiene por objeto restringir la concurrencia, siempre que las soluciones ofertadas acrediten de manera fehaciente una equivalencia funcional y operativa real.

A estos efectos, únicamente se considerarán equivalentes aquellas soluciones que:

- Cumplan íntegramente las prescripciones técnicas y funcionales del pliego.
- Permitan la integración efectiva con la instalación existente.
- Garanticen la reutilización de los modelos, configuraciones y métricas ya implantadas, sin necesidad de reprocesos, reconfiguraciones sustanciales ni desarrollos adicionales significativos.
- No impliquen la sustitución del entorno tecnológico existente ni una alteración sustancial de los procesos operativos actualmente en uso.

Por todo ello, la referencia a la solución del fabricante Pentera en el presente Sistema Dinámico de Adquisición se considera técnicamente necesaria y proporcionada para asegurar la continuidad del servicio y la adecuada ejecución del contrato.



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

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

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

D./D^a:....., con D.N.I. n^o:....., 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^o:....., Población:....., Provincia:....., y código postal:.....

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

DECLARA

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

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



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

*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



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

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

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

Vista la declaración responsable de cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos (RGPD) 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.



La autenticidad de este documento se puede comprobar en <https://gestiona.comunidad.madrid/csv> mediante el siguiente código seguro de verificación: **1055154624058134589260**

ANEXO VII ENTREGAS PARCIALES

NO APLICA

<i>Entrega 1: No Aplica</i>	<i>No Aplica</i>	<i>No Aplica</i>
-----------------------------	------------------	------------------

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: No aplica

Acuerdos de nivel de servicio:

Id.	Nombre	Descripción del indicador	Valor
ANS_01	<i>Tiempo de respuesta</i>	<i>Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha empezado a trabajar en su resolución.</i>	<i>No aplica</i>
ANS_02	<i>Tiempo de resolución de incidencia leve</i>	<i>Tiempo transcurrido desde el final del tiempo de respuesta hasta que el equipo de soporte ha solucionado la incidencia.</i>	<i>No aplica</i>
ANS_03	<i>Tiempo de resolución de incidencia grave</i>		<i>No aplica</i>
ANS_04	<i>Tiempo de resolución de incidencia crítica</i>	<i>No incluye el tiempo necesario para la aprobación por el Responsable del Contrato Específico.</i>	<i>No aplica</i>
...



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055154624058134589260**

ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN

D., con DNI o documento equivalente en caso de extranjeros o. pasaporte nº....., en su propio nombre, o como representante legal de la empresa adjudicataria del CONTRATO ESPECÍFICO Nº del SISTEMA DINÁMICO PARA EL SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (SDA 25/2021; Expediente 2022/48), pongo en conocimiento del órgano de contratación, a los efectos del artículo 215.2.b) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), que, para la prestación indicada, se subcontrata con la/s siguiente/s entidad/es:

(Indicar:

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

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

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

- **Declaración responsable** de los subcontratistas de no hallarse incurso en prohibición de contratar, conforme el art. 71 de la LCSP.¹²
- **Certificación positiva** de la Agencia Estatal de Administración Tributaria de hallarse los subcontratistas al corriente en el cumplimiento de las obligaciones tributarias o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.
- **Certificación positiva** de la Tesorería General de la Seguridad Social de hallarse los subcontratistas al corriente de sus obligaciones con la Seguridad Social o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a de de

Firmado electrónicamente

¹² La declaración responsable deberá formularse en los siguientes términos “Que ni el firmante de la declaración, ni la persona física/jurídica a la que representa, ni ninguno de sus administradores o representantes se hallan incurso en supuesto alguno a los que se refiere el artículo 71 de la LCSP.”



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

Don/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:

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

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

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



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

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

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

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

Acredita la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT (declaración censal 036 o 037¹³ o documento equivalente de las Administraciones Forales) que incluye la actividad objeto del contrato basado conforme a lo previsto en el artículo 8 apartado 2 de la Orden HFP/1030/2021, de 29 de septiembre).

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

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

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

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

....., XX de de 202X

Fdo.

Cargo:

¹³ Estas declaraciones podrán obtenerse por las empresas en la sede de la AEAT en el siguiente enlace <https://sede.agenciatributaria.gob.es/Sede/tramitacion/G322.shtml> . Si tienen dudas llamen al teléfono general de consultas de la Agencia Tributaria o al 060.



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

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

En todos los contratos específicos financiados¹⁴ por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiables, estableciéndose las siguientes **obligaciones**:

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

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

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

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

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

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

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



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: **1055154624058134589260**

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

1. RÉGIMEN JURÍDICO APLICABLE

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

La financiación del contrato se efectúa con cargo a fondos del Mecanismo de Recuperación y Resiliencia de la Unión Europea – Next Generation EU- establecido por el Reglamento (UE) 2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, y regulado según el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.

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

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

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

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

Etiquetado verde	Etiquetado digital
<i>Incluir %</i>	<i>Incluir %</i>

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**:

(Indicar obligaciones específicas o indicar que no existen obligaciones específicas)

- b) Obligaciones al componente/inversión por el **etiquetado digital**:

(Indicar obligaciones específicas o indicar que no existen obligaciones específicas)

- 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.

Prestación	Objetivo	Condición
<i>i.e. Servidores y sistemas de almacenamiento</i>	<i>Mitigación cambio climático Transición a una economía circular</i>	<i>Los equipos que se utilicen cumplirán los requisitos relacionados con el consumo energético establecidos de acuerdo con la Directiva 2009/125/EC</i>



<i>i.e. Servidores y sistemas de almacenamiento</i>	<i>Transición a una economía circular</i>	<i>Los equipos no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE.</i>
<i>Incluir otras si proceden....</i>		

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).

