

**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

**CONTRATACIÓN DE UNA SOLUCIÓN DE PROTECCIÓN DE
DIRECTORIO ACTIVO, ATAQUES BASADOS EN IDENTIDAD Y
VULNERABILIDADES DE PROTOCOLOS DE AUTENTICACIÓN EN EL
SERVICIO MADRILEÑO DE SALUD**

Lote 4 - Software de ciberseguridad

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

TÉRMINOS Y CONDICIONES

1. ORGANISMO, DESTINATARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DEL CONTACTO.....	3
2. LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO.....	3
2.1. Lote, título y objeto	3
2.2. Características principales de las prestaciones.....	4
2.3. Tratamiento de datos de carácter personal por parte del adjudicatario.....	5
2.4. Categorización conforme al Esquema Nacional de Seguridad (ENS).....	5
2.5. Tratamientos de datos personales para los programas en modalidad de nube.....	6
3. DURACIÓN DEL CONTRATO.....	6
3.1. Fecha de inicio de la ejecución.....	6
3.2. Plazo de entrega de las licencias.....	6
3.3. Plazo de ejecución del contrato.....	7
3.4. Prórroga del contrato específico.....	7
4. VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN.....	7
4.1. Presupuesto de licitación y aplicaciones presupuestarias.....	7
4.2. Determinación del precio del contrato.....	9
4.3. Tramitación del expediente (a efectos presupuestarios)	10
4.4. Modificación del contrato específico.....	10
4.5. Valor estimado.....	11
4.6. Contrato financiado con cargo al presupuesto de la Unión Europea.....	11
5. LUGAR Y CONDICIONES DE LA ENTREGA.....	12
6. INCOMPATIBILIDADES PARA LA LICITACIÓN.....	12
7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN.....	13
7.1. Ponderación de los criterios de adjudicación.....	13
7.2. Fórmula aplicable al criterio precio.....	13
7.3. Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio.....	14
7.3.1. Criterios evaluables automáticamente mediante fórmulas.....	14
7.3.2. Fórmulas para la evaluación automática de los criterios.....	18
7.4. Criterios cuya cuantificación depende de un juicio de valor.....	19
7.4.1. Criterios y ponderación.....	19
7.4.2. Método de valoración y documentación.....	19
8. OFERTAS ANORMALMENTE BAJAS.....	20
9. CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA.....	21
9.1. Obligaciones generales.....	21
9.2. Otras condiciones de ejecución del contrato.....	21
9.3. Obligaciones de seguridad en cumplimiento del ens.....	22
9.4. Obligaciones relativas al cumplimiento de las condiciones de los programas ofertados en modalidad de nube cuando exista tratamiento de datos personales.....	23



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

10. PAGO Y FACTURACIÓN.....	24
10.1. Pago del precio.....	24
10.2. Condiciones de presentación de las facturas.....	24
11. GARANTÍA DE LOS BIENES.....	25
12. PENALIDADES.....	26
12.1. Penalidades fijadas en el sistema dinámico de adquisición.....	26
12.2. Fórmula para la aplicación de penalidades.....	27
13. CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	27
14. FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS.....	27
ANEXO I PRESCRIPCIONES TÉCNICAS.....	29
I.1. Requisitos funcionales de los programas a suministrar.....	29
I.2. Requisitos no funcionales de los programas a suministrar.....	33
I.3. Periodo de vigencia y modalidad de licenciamiento.....	35
I.4. Requisitos de seguridad de los programas en la nube.....	38
ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO.....	39
II.1. Servicios de instalación avanzada de los programas a suministrar.....	39
II.2. Servicios de soporte de los programas a suministra.....	41
II.2.1. Dimensionamiento del servicio.....	41
II.2.2. Acuerdos de nivel de servicio.....	41
II.3. Requisitos de los perfiles profesionales.....	42
ANEXO III TRATAMIENTO DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS.....	43
III.1. Tratamientos de datos y finalidad de los tratamientos.....	43
III.2. Medidas técnicas y organizativas.....	43
ANEXO IV MODELO DE DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.....	44
ANEXO V MANIFESTACIÓN DE CONFORMIDAD DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS DEL ORGANISMO DESTINATARIO.....	45
ANEXO VI ENTREGAS PARCIALES.....	46
ANEXO VII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO.....	47
ANEXO VIII MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN.....	50
ANEXO IX DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DEL CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA.....	51
ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA.....	53
a. Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea.....	53
b. Obligaciones generales aplicables a los contratos financiados con cargo al PRTR.....	55

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

Organismo destinatario

Unidad proponente: CM – DIRECCIÓN GENERAL DE SALUD DIGITAL

Centro directivo: CONSEJERÍA DE DIGITALIZACIÓN

Departamento/organismo: DIRECCIÓN GENERAL DE SALUD DIGITAL (DGSD)

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

Nuria Ruiz Hombrebueno. Directora General de Salud Digital, Consejería de Digitalización.

Datos de contacto:

Dirección Postal: C/ Melchor Fernández Almagro 1, 28029 - Madrid

Correo electrónico: dgsd@salud.madrid.org

Teléfono: 913442339

Órgano de Contratación:

- Servicio Madrileño de Salud

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: Contratación de una solución de protección de directorio activo, ataques basados en identidad y vulnerabilidades de protocolos de autenticación en el Servicio Madrileño de Salud.

Objeto del contrato:

El objeto del contrato es la adquisición, por un periodo de 36 meses, de una solución software para la protección del Directorio Activo (AD) del Servicio Madrileño de Salud (SERMAS). Esta solución debe:

1. Dotar al SERMAS de visibilidad en tiempo real respecto al estado de salud, desde el punto de vista de la seguridad, de su entorno de Directorio Activo, mostrar su nivel de exposición a amenazas, recomendar líneas de mejora y mejores prácticas y evaluar el nivel de exposición al riesgo.
2. Detectar, proteger y bloquear intentos de ataque basados en vulnerabilidades de protocolos de autenticación.

Proporcionar capacidades de análisis de comportamiento de todos los usuarios (identidades) de Directorio Activo, permitiendo definir niveles de riesgo en tiempo real, así como establecer políticas de detección, cambio de contraseña, bloqueo y acceso condicional a recursos corporativos.

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 expediente.

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

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

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

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

2.3 TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DEL ADJUDICATARIO

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

☐ **NO. Cláusula aplicable para “Protección de datos sin acceso a datos personales”.** El contrato NO requiere tratamiento de datos personales por parte del adjudicatario.

☒ **SÍ. Cláusula aplicable para “Protección de datos con acceso a datos personales”.** El contrato SI requiere tratamiento de datos personales por parte del adjudicatario. La finalidad para la que se ceden los datos es:

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: categoría
- Sistema: categoría
-

URL donde se publica la certificación o declaración de conformidad (art. 38.2 del ENS):

☒ 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:

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.

3. DURACIÓN DEL CONTRATO

3.1. FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

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

3.2. PLAZO DE ENTREGA DE LAS LICENCIAS

- ☒ No admite entregas parciales. **Plazo máximo** de entrega³: 15 días naturales contados a partir de la fecha de inicio de ejecución del contrato.
- ☐ Deben realizarse entregas parciales. Los plazos y lugar de las entregas se detallan en el **Anexo VI**.

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

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, ncluido 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: 1 mes
- ☐ 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):
- ☐ XX días/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 (€)
3.620.000,00 €	760.200,00 €	4.380.200,00 €

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. 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.

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
SUMINISTRO			
Suministro de licencias (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	3.554.803,29 €	746.508,69 €	4.301.311,98 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	65.196,71 €	13.691,31 €	78.888,02 €
Servicio de soporte, a prestar por el adjudicatario			
TOTAL	3.620.000,00 €	760.200,00 €	4.380.200,00 €

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. Las ofertas que presenten los licitadores no podrán superar el importe presupuestado de los servicios de soporte. Se excluirán 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 Servicio *Madripleño de Salud*, Centro de Gestión Servicios *Centrales*, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	Anualidad 2023	TOTAL
G/311P/64001 (Software)	4.301.311,98 €	4.301.311,98 €
G/311P/22703 (Servicios)	78.888,02 €	78.888,02 €

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	54.787,15 €
Resto costes directos	2.987.229,66 €
Costes indirectos + Gastos generales + Beneficio industrial	577.983,19 €
Total sin IVA	3.620.000,00 €

Justificación: Los precios marcados en este documento están basados en la solicitud de ofertas previas al mercado por los suministros solicitados junto con la garantía asociada a dicho suministro. Los gastos generales se han estimado en un 13 % y el beneficio industrial en un 6 %, en base a la previsión establecida en el artículo 131 del RGLCAP.

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

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

El convenio colectivo sectorial de aplicación en los términos indicados es el XVIII Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública, publicado en el BOE del día 26 de julio de 2023 mediante Resolución de 13 de julio de 2023, de la Dirección General de Trabajo, por la que se registra y publica el citado Convenio. No consta que exista diferencia por género en el Convenio colectivo que resulta de aplicación

Costes de personal							
Perfiles	Dedicación	Salario Base	Especialización tecnológica (49)	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 30%
1 JEFE DE PROYECTO (RESPONSABLE DEL SERVICIO) Consultoría desarrollo y sistemas (AREA 3 Grupo A Nivel 1)	100%	28.284,54 €	13.859,42 €	42.143,96 €	42.143,96 €	42.143,96 €	54.787,15 €

Si bien resulta de aplicación el convenio sectorial, en el presente servicio se requiere una cualificación superior debido a la alta especialización técnica y experiencia requerida en la arquitectura tecnológica y herramientas necesarias para ejecutar los trabajos descritos en este documento con los plazos y calidad exigidos por la DGSD. Dada la naturaleza del entorno y la criticidad del mismo, el jefe de proyecto debe tener cualificación y experiencia en el ámbito de la gestión de la protección de Directorio Activo. Así mismo, dadas las características de la arquitectura tecnológica para la gestión de sistemas críticos, debe de disponer de la cualificación y experiencia en auditoría de directorio activo de entornos de alta disponibilidad. Se estima un porcentaje de especialización técnica del 49% para el perfil solicitado, tal y como se refleja en la anterior tabla de costes de personal.

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 específico⁵:

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.

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



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

4.5. VALOR ESTIMADO

Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **3.620.000,00 euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	3.620.000,00 €
Importe máximo por modificación prevista, sin IVA	
TOTAL	3.620.000,00 €

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: **NEXT GENERATION EU - MECANISMO DE RECUPERACIÓN Y RESILIENCIA. PLAN DE RECUPERACIÓN, TRANSFORMACION Y RESILIENCIA/POLÍTICA PALANCA IV/COMPONENTE 11/INVERSIÓN 3.**

Código de operación/Proyecto/Iniciativa: **GRUPO 1.1 CIBERAP**

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

5. LUGAR Y CONDICIONES DE LA ENTREGA

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

- Dirección Postal: Dirección General de Salud Digital. Consejería de Digitalización. Comunidad de Madrid. Melchor Fernández Almagro, 1 – 28029 Madrid.
- Correo electrónico: dgsd@salud.madrid.org
- Teléfono: 913442261 / 913442292
- Fax:

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 VI**.

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:

☐ Existen incompatibilidades por causa de la naturaleza de los trabajos.

7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN ⁶

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
60 puntos	40 puntos

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

RE 1. Criterios que dependen de juicio de valor	SOBRE 2.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 2.2. Precio

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)

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

☒ 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)

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.

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

7.3.1. CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS

CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓN, según apartado 7.5
CA1 – Certificaciones oficiales del equipo técnico del licitador	10	Sí/No
CA2 – Mejoras en el soporte a la transferencia de conocimiento. Certificaciones oficiales ofrecidas por el fabricante al Organismo	10	Sí/No
CA3 – Mejoras en el soporte y mantenimiento del fabricante. Tiempo de respuesta a incidencias	5	Sí/No
CA4 – Mejoras en el soporte y mantenimiento del fabricante. Gestor técnico de cuenta (Technical Account Manager – TAM)	5	Sí/No
CA5 – Mejoras en la disponibilidad de la plataforma ofertada.	5	Sí/No
CA6 – Mejoras en la respuesta a incidentes de la plataforma ofertada. Capacidades de análisis forense de la solución	10	Sí/No
CA7 – Mejoras en el soporte a la respuesta a incidentes de seguridad. Capacidad en línea de inspección profunda de paquetes de tráfico de Directorio Activo	15	Sí/No

Se definen los siguientes:

CA1 – Certificaciones oficiales del equipo técnico del licitador.

Se valorará en este criterio las garantías de servicio y seguridad ofrecidas por el equipo técnico del prestatario del servicio basadas en certificaciones oficiales de seguridad expedidas por el fabricante de la plataforma de seguridad ofertada. Los técnicos del equipo del licitador que disponen de las certificaciones deberán ser los técnicos que van a intervenir en la ejecución del contrato.

Se obtendrá la máxima puntuación del criterio si la empresa licitadora dispone de al menos un perfil técnico que disponga de certificación oficial del fabricante en administración avanzada de la plataforma de seguridad ofertada y un perfil técnico que disponga de certificación oficial del fabricante en hunting o búsqueda activa de amenazas utilizando la plataforma de seguridad ofertada.

Peso (puntos): 10

CA2 – Mejoras en el soporte a la transferencia de conocimiento. Certificaciones oficiales ofrecidas por el fabricante al Organismo.

Se valorará en este criterio las mejoras en el soporte a la transferencia de conocimiento. En concreto se valorarán los cursos y certificaciones, ofrecidos para personal del Organismo, en administración y operación de la plataforma tecnológica ofertada:

Se obtendrá la máxima puntuación del criterio si se incluye en la propuesta un curso (de al menos 10 horas de duración) y examen de certificación del fabricante en administración de la plataforma para 7 personas.

Peso (puntos): 10

CA3 – Mejoras en el soporte y mantenimiento del fabricante. Tiempo de respuesta a incidencias.

Se valorará en este criterio la mejora del soporte y mantenimiento del fabricante relacionado con la reducción del tiempo acordado de respuesta de incidencias:

Se obtendrá la máxima puntuación del criterio si se oferta en la propuesta una reducción del tiempo acordado de respuesta a incidencias de Severidad 1 (primer nivel) de 1 hora.

Peso (puntos): 5



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

CA4 – Mejoras en el soporte y mantenimiento del fabricante. Gestor técnico de cuenta (Technical Account Manager – TAM).

Se valorará en este criterio la mejora del soporte y mantenimiento del fabricante relacionado con la disponibilidad de un gestor técnico de cuentas (TAM – Technical Account Manager) que ayude con los casos en curso y la transferencia de conocimiento:

Se obtendrá la máxima puntuación del criterio si se oferta en la propuesta un gestor técnico de cuenta (Technical Account Manager – TAM) proporcionado por el fabricante de la plataforma de seguridad ofertada, en idioma español.

Peso (puntos): 5

CA5 – Mejoras en la disponibilidad de la plataforma ofertada.

Se valorará en este criterio las mejoras en la disponibilidad por encima del mínimo exigido (99,9 %):

Se obtendrá la máxima puntuación del criterio si la plataforma propuesta garantiza una disponibilidad del 99,9 %.

Peso (puntos): 5

CA6 – Mejoras en la respuesta a incidentes de la plataforma ofertada. Capacidades de análisis forense de la solución.

Se valorará en este criterio las mejoras en las capacidades de la solución en la respuesta a incidentes. En concreto se valorarán las capacidades de la solución propuestas a mejorar las acciones orientadas a la respuesta a incidentes, incluyendo la capacidad de recopilar información, objetos y artefactos de seguridad del Directorio Activo:

Se obtendrá la máxima puntuación del criterio si la herramienta propuesta dispone de la capacidad solicitada en el criterio de adjudicación.

Peso (puntos): 10



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

CA7 – Mejoras en el soporte a la respuesta a incidentes de seguridad. Capacidad en línea de inspección profunda de paquetes de tráfico de Directorio Activo.

Se valorará en este criterio la capacidad de la herramienta propuesta en la inspección profunda de paquetes de tráfico de Directorio Activo en línea. Entendiéndose esta como la inspección profunda de paquetes de tráfico de Directorio Activo en tiempo real y de forma proactiva, es decir, no basada en el análisis de logs o información de procesos que ya han ocurrido:

Se obtendrá la máxima puntuación del criterio si la herramienta propuesta dispone de la capacidad solicitada en el criterio de adjudicación.

Peso (puntos): 15

7.3.2. FÓRMULAS PARA LA EVALUACIÓN AUTOMÁTICA DE LOS CRITERIOS

Función **Maximizar**:

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

Donde:

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

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

Función Minimizar:

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

Donde:

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

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

Función Sí/No (maximizar binario):

$$X_i = P$$

Donde:

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

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR**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: No aplica.
 - ☒ 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: 25%.

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 existen otras condiciones.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

9.3. OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

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

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

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

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

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

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

Si se ha indicado en el apartado 2.2 que los programas objeto del suministro deben procesar o almacenar datos de carácter personal conforme a lo dispuesto en el **Reglamento (UE) 2016/679**, en adelante RGPD, y en la **Ley Orgánica 3/2018**, o tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, conforme a lo dispuesto en la **Directiva (UE) 2016/680** y la **Ley Orgánica 7/2021**, sólo se aceptarán nubes cuyos proveedores de nube encargados del tratamiento se encuentren establecidos y realicen las operaciones principales de tratamiento en la UE/EEE, admitiéndose transferencias a terceros países u organizaciones internacionales siempre que el proveedor de nube establecido en la UE/EEE ofrezca garantías adecuadas conforme a lo previsto en el Capítulo V del RGPD⁷.

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

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.

⁷ La Comisión Europea ha adoptado decisiones de adecuación con Andorra, Argentina, Canadá (operaciones comerciales sólo), Islas Faroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, República de Corea, Suiza, Reino Unido y Uruguay. Puede obtenerse información adicional actualizada en la página de la AEPD <https://www.aepd.es/es/derechos-y-deberes/cumple-tusdeberes/medidas-de-cumplimiento/transferencias-internacionales>.

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

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

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

- ☒ A la recepción del servicio, tras su cumplimiento a satisfacción de la Administración.
☐ Otra:

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:
Período 2:
Período 3:
Período 4:
☐ Otra:

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 (XAdES).

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

- Órgano de contratación: Dirección General de Racionalización y Centralización de la Contratación - E04962703.
- Órgano responsable del contrato específico (DIR3):
- Órgano gestor (DIR3):
- Unidad tramitadora (DIR3):
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3):

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.

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: Servicio Madrileño de Salud - A13003096.
- Órgano responsable del contrato específico (DIR3): Dirección General de Salud Digital - A13003096.
- Órgano gestor (DIR3): Servicio Madrileño de Salud - A13003096.
- Unidad tramitadora (DIR3): UGEP DIRECCIÓN Y SERV.GEN.SERVICIO MADRILEÑO DE SALUD - GE0016401.
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3): Intervención General de la Comunidad de Madrid - A13029032.

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

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

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 VII** 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	Apartado 12.2
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**.

12.2. FÓRMULA PARA LA APLICACIÓN DE PENALIDADES

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

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

Donde:

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

13. CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO

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

14. FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS

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

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

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

La oferta económica deberá incluir, al menos, la información en el modelo de oferta disponible en el Portal de Contratación Centralizada para el SDA 25/2022, en la siguiente dirección: https://contratacioncentralizada.gob.es/documents/11614/210125/Modelos+de+Oferta+SDA25_2022.zip/9854d53b-ca36-4840-a817-1161b3e4ee17. 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.

⁸ Las ofertas se presentarán a través de LICIT@, disponible en el Portal de la Contratación de la Comunidad de Madrid. El enlace de acceso es: https://gestion5.madrid.org:8203/sap/bc/webdynpro/sap/zfrms_wd_le_003#

⁹ Para facilitar la identificación el firmante apoderado de la empresa se deberá indicar, además de sus datos, el número de usuario apoderado de la aplicación AUNA.

La oferta técnica deberá contener la siguiente documentación:

- Relación de los programas en la modalidad de licenciamiento que se ofertan
- La información de los requisitos mínimos de los productos o referencias a las fichas técnicas o catálogos que permitan acreditar los criterios automáticos:
 - Cumplimiento de los requisitos funcionales que se describen en el apartado I.1 del Anexo I
 - Copia de las certificaciones solicitadas en los criterios.
- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
NO APLICA
- 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.

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): LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: NURIA RUIZ HOMBREBUENO
Fecha: 2023.10.26 12:57

Firmado electrónicamente (nombre y apellidos): Nuria Ruiz Hombrebueno

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

En la actualidad, el Servicio Madrileño de Salud (SERMAS) dispone de solución de Directorio Activo ampliamente implantada en su Organización. Esta infraestructura de Directorio Activo se encuentra distribuida en un número significativo de nodos (Controladores de Dominio) que dan servicio a un número aproximado de 113.000 usuarios corporativos. Mediante el Directorio Activo corporativo, se facilita la gestión de accesos a los distintos recursos IT corporativos, cuentas de usuario, equipos y objetos de Directorio.

Tal y como se indica en apartados anteriores, el objeto del contrato es la adquisición, por un periodo de **48 meses**, de una solución software para la protección del Directorio Activo (AD) del Servicio Madrileño de Salud (SERMAS). Esta solución debe:

1. Dotar al SERMAS de visibilidad en tiempo real respecto al estado de salud, desde el punto de vista de la seguridad, de su entorno de Directorio Activo, mostrar su nivel de exposición a amenazas, recomendar líneas de mejora y mejores prácticas y evaluar el nivel de exposición al riesgo.
2. Detectar, proteger y bloquear intentos de ataque basados en vulnerabilidades de protocolos de autenticación.
3. Proporcionar capacidades de análisis de comportamiento de todos los usuarios (identidades) de Directorio Activo, permitiendo definir niveles de riesgo en tiempo real, así como establecer políticas de detección, cambio de contraseña, bloqueo y acceso condicional a recursos corporativos.

El alcance de cuentas de Directorio Activo a cubrir mediante este contrato es de **113.000 cuentas activas de Directorio Activo, por lo que deberá incluirse en la propuesta licenciamiento suficiente para cubrir este alcance.**

En cuanto a los requisitos técnicos y funcionalidades de la solución de seguridad y control de directorios activos, se deberán tener en cuenta las siguientes premisas:

Características técnicas generales con las que debe contar la solución de manera obligatoria:

- La solución debe contar con un modelo de arquitectura multi-entidad, incorporando dependencias e interrelaciones entre las diferentes gerencias territoriales que componen el Servicio de Salud de la Comunidad de Madrid.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

A través de la arquitectura multi-entidad se garantizará la separación de la información por cada una de las sedes del Servicio de Salud, así como la gestión completa desde una sede principal.

- La herramienta deberá ser capaz de gestionar un sistema multiusuario que facilite realizar perfilado de usuarios en base a módulos/funciones.
- El acceso a la consola de gestión será mediante interfaz basada en entorno web multiplataforma/navegador, con diseño responsive y alto nivel de usabilidad. Los navegadores soportados serán al menos Microsoft Edge y Google Chrome.
- La solución deberá permitir el acceso a todos los módulos de la herramienta a los que tenga acceso (permisos) desde una misma sesión, sin que requiera del usuario múltiples autenticaciones.
- La solución deberá tener capacidad de incorporar mecanismos que ayuden y dinamicen a los profesionales especializados o no en esta cuestión: alertas, recordatorios, sugerencias, etc.
- La herramienta debe disponer de servicios web y/o APIs para la explotación de información desde terceros sistemas del Servicio de Salud.
- La solución debe proporcionar una API rica y robusta para integración con herramientas de terceros.
- Todo el equipamiento desplegado deberá seguir y cumplir con los requerimientos de sistemas y seguridad marcados por el Departamento TIC del Servicio de Salud.

Funcionalidades y características de seguridad con las que debe contar la solución de manera obligatoria:

- La plataforma debe facilitar la comunicación de alertas de detección en tiempo real, y proporcionar informes y cuadros de mando en tiempo real.
- Debe mostrarse en la consola una puntuación de riesgo de las amenazas en tiempo real. Esta puntuación de riesgo debe ser dinámica y evolucionar en tiempo real en función de las distintas métricas que se utilicen para su cálculo, permitiendo a los administradores conocer en todo momento el estado y severidad de amenazas y ataques.
- La solución propuesta deberá disponer de capacidad de retención y análisis libre de los eventos de los directorios activos incluidas la creación y modificación de GPOs. La capacidad de retención de eventos será de 90 días.
- La plataforma debe proporcionar un registro de auditoría de la actividad de los usuarios incluidas las tareas de gestión y respuesta a incidentes. Esta información de auditoría debe ser accesible desde la propia interfaz o a través de API. Debe contener al menos la siguiente información: creación de administradores, cambios de permisos, login a la plataforma, actividad durante la sesión, conexiones a host, comandos ejecutados, inicio y duración de la sesión.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

- La solución proporcionada debe proporcionar un score de riesgo por cada usuario indicando al menos indicadores tales como: compromiso de la contraseña indicando el motivo exacto, inactividad, último cambio de contraseña, calidad y robustez de la contraseña, permisos, ...
- La solución propuesta deberá permitir la inspección de tráfico realizada hacia los directorios.

Funcionalidades específicas de **protección contra ataques basados en identidad** con las que debe contar la solución de manera obligatoria:

- Se requieren capacidades de seguridad vinculadas a la protección de entornos de Directorio Activo, así como detección de ataques basados en vulnerabilidades de protocolos de autenticación.
- Específicamente se requieren capacidades de seguridad vinculadas a la protección de entornos de Directorio Activo, así como detección de ataques basados en vulnerabilidades de protocolos de autenticación. Adicionalmente, se requieren funcionalidades que permitan detectar y bloquear el uso ilícito de credenciales, intentos de suplantación de identidad, propagación lateral, acceso a recursos y activos críticos.
- Se requiere que las capacidades de detección, protección, bloqueo y prevención puedan aplicarse en arquitecturas de Directorio Activo en formato on-premise (infraestructura, servicios de directorio activo y controladores de dominio en entornos propios del Organismo), cloud (servicios e infraestructura de Directorio Activo ubicados en entorno de nube pública) o híbridos (convivencia de las dos modalidades anteriores).
- No se considerarán válidas soluciones que únicamente proporcionen capacidades de monitorización o detección sin poder aplicar funcionalidades de protección, prevención o bloqueo (enforcement de políticas de seguridad definidas). Estas capacidades de detección, protección y bloqueo deben poder aplicarse de forma completa independientemente de la arquitectura de Directorio Activo.
- La solución debe restringir y bloquear todas las operaciones de una cuenta marcada como honeytoken (cuentas señuelo para identificar atacantes).
- La solución propuesta debe permitir la definición e implantación de políticas como mínimo de detección, bloqueo, forzado de cambio de contraseña o acceso condicional (mediante la integración con herramientas de autenticación de doble factor) basadas en desviación de comportamiento respecto a la línea base de comportamiento de usuario.
- La solución debe posibilitar el análisis de comportamiento del usuario para detectar amenazas con una respuesta contextual automatizada que redirija el comportamiento de riesgo del usuario y detenga proactivamente las amenazas. Se requiere que la solución disponga de funciones de aprendizaje automático del entorno, permita hacer seguimiento de los comportamientos a lo largo del tiempo y aplicar políticas flexibles que puedan adaptarse automáticamente a medida que cambien las circunstancias del entorno. a. La solución debe realizar detección/bloqueo basado en comportamiento anómalo UEBA.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

- La plataforma, tras la detección de riesgos vinculados a la identidad, debe ofrecer información sobre recomendaciones y buenas prácticas de operación/administración del directorio que permitan reducir la superficie de exposición al riesgo.
- La solución debe mostrar información de usuarios con credenciales comprometidas mediante la búsqueda en las principales fuentes de datos públicos. Adicionalmente, la solución debe disponer de la capacidad para los analistas/operadores de añadir contraseñas para verificar si están siendo utilizadas por las identidades monitorizadas (custom password dictionary).
- La solución debe disponer de capacidades de detección de exploits específicos utilizados en entornos de identidad con el objetivo de obtener credenciales o realizar login de forma anómala o ilícita.
- La solución propuesta debe poder enriquecer las capacidades de threat hunting permitiendo realizar consultas en la información de telemetría relacionadas con atributos y eventos del tráfico de autenticación, atributos de usuarios, dispositivo, métodos de acceso, cambios en la cuenta, etc. (sin impacto en rendimiento de estos sistemas).
- Para supervisar los controladores de dominio, la solución capturará y analizará el tráfico de red hacia los controladores de dominio en busca de amenazas y ataques. La solución obtendrá información sobre la red, permitiendo la detección de anomalías y generando alertas de las actividades sospechosas. Se requiere que las capacidades de detección y prevención detalladas en los requisitos anteriores puedan aplicarse en línea, es decir, en tiempo real, no siendo válidas soluciones que apliquen las políticas de detección y prevención a posteriori basadas en un análisis posterior de información o logs de los sistemas de gestión de identidad (controladores de dominio).

Adicionalmente, considerando la relevancia y criticidad especial de las infraestructuras de sistemas que sustentan los sistemas de identidad de Directorio Activo (Controladores de Dominio), es necesario que estas funcionalidades específicas de seguridad orientadas a la protección de identidades puedan convivir sin impacto en rendimiento de estos sistemas.

Capacidades de orquestación y automatización con las que debe contar la solución de manera obligatoria:

- Se requiere que la solución permita realizar automatizaciones y orquestaciones de tareas y respuestas automáticas en base a criterios de telemetría y/o detección. Los licitadores expondrán en su propuesta cómo se implementan estas funcionalidades y sus capacidades, referidas a casos de uso.
- Inclusión de las capacidades de automatización y orquestación en la misma consola o interfaz, de acuerdo con los requisitos sobre la arquitectura de la solución, entendiéndose ésta el portal web único en el que se recojan todas las capacidades.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

A efectos de verificación de la interfaz o consola única, no se considerarán válidas soluciones que requieran vincular, enlazar o integrar distintas plataformas o aplicaciones web, dominios o consolas para cubrir las funcionalidades requeridas o aquellas que integren estas consolas en un portal de aplicaciones.

Capacidades de automatización de la plataforma deben ser las siguientes:

- Capacidad de creación de flujos de trabajo y playbooks de automatización mediante interfaz visual en la propia plataforma. Los usuarios administradores de la plataforma deben disponer de permisos para la creación/edición de estos playbooks.
- Contar con disparadores de acciones.
- Capacidad de establecer condiciones tanto de forma secuencial como paralela.
- Capacidad de establecer acciones de respuesta.
- Debe poder disponer de un versionado de los playbooks o flujos de trabajo creados.
- Debe proporcionar un log de ejecución del flujo de trabajo creado.

Funcionalidades de reporte con las que debe contar la solución de manera obligatoria:

- La solución deberá contar con capacidades de reporting avanzadas que permitan ver la evolución del organismo, faciliten el conocimiento general y de detalle de la situación, así como incorporación de mecanismos de alerta.
- La solución debe contar con la posibilidad de programar cuadros de mando e informes en base a la información tratada y las necesidades del Servicio de Salud.
- La solución debe disponer de mecanismos y conservación de trazabilidad, generación de informes, plantillas, control de avisos y notificaciones.
La solución debe permitir programar informes mensuales diferenciados por centros e incluso por tipos de usuarios finales de la herramienta.
- La solución deberá contar con la posibilidad de configurar y remitir alertas antes la detección de nuevos riesgos y amenaza en base a los criterios definidos por el Servicio de Salud.
- La solución deberá permitir la retención de información por un mínimo de 90 días.

I.2 REQUISITOS NO FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

Arquitectura de la solución

A continuación, se definen los requisitos mínimos que se deberán tener en cuenta en lo referente a los requerimientos de arquitectura de la solución propuesta:

- Todos los requisitos de seguridad deben ser cubiertos por un único fabricante, una única tecnología y deben ser provistos desde una única interfaz o consola.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

- Las tareas de gestión, mantenimiento y actualizaciones de la plataforma deben realizarse de forma transparente para el servicio, sin ninguna indisponibilidad del servicio o inactividad total o parcial.
- La solución debe ser autoescalable y no debe requerir el mantenimiento de ninguna infraestructura garantizando la misma calidad de servicio independientemente de la demanda.
- La solución debe disponer de flexibilidad para absorber picos de demanda estacionales y puntuales (incremento de cuentas de usuario por encima del alcance solicitado en el expediente) durante periodos limitados de tiempo sin producir ninguna limitación en el servicio o indisponibilidad de éste.
- La solución debe disponer de control de acceso con doble factor de autenticación, soportar SSO (SAML 2.0), múltiples usuarios y diferentes roles para permitir el acceso a diferentes ámbitos o funcionalidades.
- Las comunicaciones entre la consola y los agentes tendrán que ser cifradas.
- En caso de que la solución ofertada requiera de agente, las características del agente deberán cumplir con los siguientes requisitos obligatorios:
 - Permitir un despliegue sencillo de la solución.
 - Minimizar el impacto en rendimiento en el servidor con el rol de controlador de dominio final.
 - Que su implantación no suponga una interrupción en los servicios productivos.
 - Un único agente instalado en los Controladores de Dominio no siendo válidas soluciones que requieran distintos agentes para proporcionar todas las funcionalidades solicitadas.
 - Debe poder convivir con los sistemas de protección de puestos (Antivirus/EPP/EDR) existentes manteniendo todas sus funcionalidades, no debiendo producirse incompatibilidades o requerimientos de desconexión de capacidades de la solución propuesta o de la solución de protección de puesto existente en el servidor.
 - El agente a desplegar en los puestos de usuario o servidor debe poder convivir con las soluciones microCLAUDIA y CLAUDIA del CCN, manteniendo todas sus funcionalidades, no debiendo producirse incompatibilidades o requerimientos de desconexión de capacidades de la solución propuesta o de la solución de protección de puesto.
 - La instalación completa del agente en cada uno de los Controladores de Dominio debe poder hacerse sin reinicio y sin intervención del usuario.
 - Se requiere una solución que minimice las dependencias con el software y middleware del servidor. Esto es, soluciones que, para su instalación completa con todas las funcionalidades requeridas activas, necesiten los mínimos requisitos del host en cuanto a parches, drivers, service packs, bibliotecas del sistema y otros elementos software y no hagan uso de librerías del sistema para aplicar funcionalidades de protección. Los licitadores tendrán que indicar la lista de requisitos necesarios y ésta estar contrastada con información oficial del fabricante.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

- El consumo total de los procesos vinculados al agente de la solución en modo monitorización debe ser inferior al 3% de la/las CPUs físicas o virtuales. Este consumo máximo de CPU debe ser garantizado no admitiéndose soluciones que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución en modo monitorización, superen el consumo máximo indicado.
- El consumo máximo de memoria RAM para el funcionamiento del producto en modo monitorización debe ser inferior a 150MB (Mega Bytes). No se admitirán soluciones que superen este consumo.
- El tamaño en disco del instalador del agente no debe ser superior a 250 MB.
- El agente a instalar en servidores debe ser compatible con infraestructuras físicas y virtuales.
- Deberá contar con capacidades de securización basadas en tokens para controlar, permitir o bloquear la instalación y desinstalación del agente en los servidores. De esta forma, en los casos que se consideren necesarios, aunque se disponga del paquete de instalación o de permisos para el lanzamiento de scripts de despliegue, deberá disponerse de un token específico para poder enlazar un endpoint a la plataforma. Igualmente, debe disponerse de un token específico para poder realizar la desinstalación del agente.
- El agente deberá contar con medidas de protección para la desinstalación.
- La instalación del agente debe permitir incluir la parametrización para arquitecturas de red y seguridad basadas en proxy.

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Vigencia de las licencias: 4 años.

Programa	Periodo de vigencia del licenciamiento
Conjunto de programas Software para el cumplimiento de las funcionalidades de la plataforma de auditoría de DA solicitada en este documento.	4 años

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



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Programa	Derechos durante la vigencia de las licencias
Detección y respuesta a amenazas para DA	<ul style="list-style-type: none">• Derecho de uso: <i>por usuario nominal activo del DA.</i>• Derecho de actualización: <i>parches de seguridad, parches funcionales, y nuevas versiones.</i>• Derecho de acceso a documentación del producto.• Derecho de consulta y resolución de problemas relacionados con el software. Horario: 9x5 con 1 día de respuesta. En casos de fallo grave del software, 24x7 con 4 horas de respuesta.• Definición de severidades:<ul style="list-style-type: none">○ Severidad 1 (Primer nivel): Error crítico que inhabilita el funcionamiento del producto completamente, para el que no existe solución alternativa (workaround) y tiene un impacto claro y significativo en las operaciones de la instalación. Como consecuencia de este error, la operación del producto está parada en el sistema de producción. De igual forma, se tratarán como incidencia de nivel 1 aquellas incidencias que frenen la puesta en marcha del producto en el entorno de Producción. Los problemas de severidad 1 deben afectar a los entornos de producción (quedan específicamente excluidos los problemas en los entornos de desarrollo y pruebas).○ Severidad 2 (Segundo nivel): Error crítico para el que existe solución alternativa o error no-crítico que afecte significativamente a la funcionalidad del producto. Los problemas de severidad 2 deben afectar a los entornos de producción (quedan específicamente excluidos los problemas en los entornos de desarrollo y pruebas).○ Severidad 3 (Tercer Nivel): Error aislado que no afecta significativamente a la funcionalidad del producto.○ Severidad 4 (Cuarto Nivel): Error benigno que no afecta a la funcionalidad del producto o consultas sobre la funcionalidad/operación del producto.Severidad 5 (Quinto Nivel): Petición de mejora del producto.

Detección y respuesta a
amenazas para DA

- Tiempos de respuesta:

Cada nivel de severidad de las incidencias descrito anteriormente tiene asociados unos tiempos de respuesta desde la recepción de la notificación del problema hasta su resolución. En el supuesto de incumplimiento de estos tiempos de respuesta, se aplicarán las penalidades indicadas en el pliego de cláusulas administrativas particulares.

En la siguiente tabla se reflejan los tiempos de respuesta para todos los niveles de severidad:

Severidad	Tiempo de respuesta	Actualización	Estimación de resolución
1	2 h. Laborables	Diaria	Trabajo continuo en el horario contratado hasta resolución
2	4 h. Laborables	Diaria	Trabajo continuo en el horario contratado hasta resolución
3	8 h. Laborables	Semanal	Lo antes posible dentro de la severidad
4	12 h. Laborables	Semanal	Lo antes posible dentro de la severidad
5	16 h. Laborables	Semanal	Lo antes posible dentro de la severidad

Donde:

- Tiempo de respuesta: Tiempo máximo que transcurre entre la recepción de la incidencia y el inicio de los trabajos para su resolución.
- Actualización: Periodo de tiempo en el que se enviarán actualizaciones al cliente del estado y nivel de progreso en la resolución de la incidencia.
- Estimación de resolución: Nivel de esfuerzo dedicado para la resolución de la incidencia. En el caso de incidencias catalogadas con severidad 1 o 2, el plazo máximo de resolución a partir del cual se aplicarán las penalidades previstas en el Pliego de Cláusulas Administrativas Particulares será de 72 horas naturales.

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

Conforme al apartado III.2.3 del Pliego de Prescripciones Técnicas, las siguientes medidas¹⁰ del RD 311/2022 (Esquema Nacional de Seguridad, ENS) aplican a los programas ofertados puestos a disposición en modo nube:

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

Asociados al suministro de licencias será necesario prestar un servicio para la transferencia de conocimiento, tanto funcional como técnico, para el correcto funcionamiento de la plataforma, la monitorización y detección de amenazas y la respuesta a incidentes.

Para la organización, coordinación y control que garantice una ejecución eficaz y eficiente del objeto del contrato, así como para la interlocución y del reporte al Organismo será necesaria la figura de una persona que desempeñe la Jefatura de Proyecto.

Este servicio estará prestado en horario 8x5, de forma deslocalizada.

Transferencia de conocimiento

El suministro se acompañará de la correspondiente transferencia de conocimiento de la plataforma suministrada, destinada a empleados del Organismo y sus entidades instrumentales dedicados a tareas de ciberseguridad.

La transferencia de conocimiento sobre la plataforma tendrá dos convocatorias en fechas a determinar con el responsable del contrato, para un mínimo de 20 asistentes cada una y con una duración mínima de 8 horas lectivas.

Las sesiones serán realizadas en las instalaciones del Organismo o bien de manera virtual.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

Se proporcionará una descripción de:

- i. Los medios técnicos y materiales propuestos, como plataformas de formación, plataforma de entrenamiento, documentación y manuales.
- ii. El personal propuesto por el licitador para impartir la transferencia de conocimiento.
- iii. La organización de los programas de transferencia de conocimiento, en cuanto a número de sesiones, modalidad virtual o presencial, nº recomendado de asistentes, contenido, horas y certificaciones oficiales que no sean del fabricante.

Hitos y entregables

Hito	Descripción hito y sus entregables	Plazo	Porcentaje de la prestación
HITO_01	<p>Fase 1: Definición del despliegue.</p> <p>En esta primera fase se mantendrán reuniones para la elaboración de un Plan Técnico de Despliegue que incluirá, al menos:</p> <ol style="list-style-type: none">1) Arquitectura del sistema. Diagramas físicos y lógicos. Identificación de proveedores involucrados y certificaciones de seguridad2) Plan detallado de puesta en marcha y configuración inicial, incluyendo estimación de tiempos para cada una de las tareas. Procedimientos de aprovisionamiento e instalación, que incluya detalle de los elementos que son necesarios para disponer del sistema totalmente operativo. Identificación de los interlocutores involucrados.3) Documentación técnica. Manuales de usuario y administración.4) Plan de explotación y mantenimiento de la plataforma. <p>El plazo máximo de entrega del Plan técnico de despliegue es de dos semanas a contar desde la fecha de formalización del contrato. Una vez aprobado el Plan técnico de despliegue el responsable del contrato autorizará el comienzo de la Fase 2.</p>	1 semana	12,5 %
HITO_02	Fase 2: Provisión y configuración inicial de la plataforma.	1 semana después de la aceptación del HITO_01	



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

HITO_03	<p>Fase 3: Despliegue.</p> <p>Incluirá el desarrollo de paquetes de software para distribuir el agente a través de las herramientas de despliegue de software del organismo, y la elaboración de los procedimientos manuales de instalación y configuración del agente para aquellos servidores con el rol de Controlador de Dominio en los que no se pueda automatizar su instalación (si los hubiera).</p>	2 semanas	25 %
HITO_04	<p>Fase 4: Transferencia de conocimiento.</p> <p>En esta fase, que se desarrollará de forma paralela a las fases 1, 2 y 3, se prestará según los requisitos establecidos en el apartado Transferencia de conocimiento.</p>	4 semanas	50 %

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

NO APLICA.

II.2.1 DIMENSIONAMIENTO DEL SERVICIO

NO APLICA.

II.2.2. ACUERDOS DE NIVEL DE SERVICIO

NO APLICA.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

II.3. REQUISITOS DE LOS PERFILES PROFESIONALES

Requisitos mínimos – Jefatura de Proyecto
TITULACIÓN
Grado en Ingeniería o equivalente en la especialidad de informática y/o comunicaciones.
FORMACIÓN TÉCNICA
<ul style="list-style-type: none">- Conocimientos acreditados en gestión y soporte de productos de seguridad del fabricante (EDR).- Conocimientos en administración de Microsoft Windows y Linux.- Conocimientos en Gestión de incidentes de seguridad.
ACTIVIDAD PROFESIONAL
<ul style="list-style-type: none">- Al menos 60 meses de experiencia en gestión de proyectos.- Al menos 36 meses de experiencia en la organización y gestión de equipos técnicos especialistas en la detección y remediación de incidencias de seguridad.- Al menos 24 meses de experiencia en proyectos de despliegue y gestión de soluciones de seguridad EDR.

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: Datos relativos al personal al servicio de la Consejería de Sanidad
- Categorías de datos personales tratados: Identificador de usuario, nombre y apellidos, correo corporativo, DNI
- Datos sensibles tratados (si procede) y restricciones o garantías aplicables: No hay tratamiento de datos sensibles.
- Naturaleza del tratamiento: Recopilación y análisis de datos.
- Finalidad(es) del tratamiento: Análisis y mantenimiento de la línea base de seguridad de los servidores y dispositivos de usuario final del organismo mediante el análisis de logs, eventos y sesiones de usuario en dichos dispositivos.
- Duración del tratamiento: Hasta la expiración del periodo de vigencia de las licencias.

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:

Dado el carácter y la finalidad de los datos recabados, las medidas técnicas y organizativas aplicadas se corresponden con las de Tipo Básico del Anexo II del ENS.

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

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

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

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

DECLARA

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



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

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

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

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

(Fecha, firma y nombre completo del representante legal)

Fdo. electrónicamente

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

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

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

MANIFIESTO

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

Indicar nombre y cargo. Firma electrónica.



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

ANEXO VI ENTREGAS PARCIALES

NO APLICA

ANEXO VII 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: 9x5 en día laborable.

Acuerdos de nivel de servicio:

Id.	Nombre	Descripción del indicador	Valor
ANS_01	Tiempo de respuesta	Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha empezado a trabajar en su resolución.	2 horas
ANS_02	Tiempo de resolución de incidencia leve	Tiempo transcurrido desde el final del tiempo de respuesta hasta que el equipo de soporte ha solucionado la incidencia. No incluye el tiempo necesario para la aprobación por el Responsable del Contrato Específico.	1 días
ANS_03	Tiempo de resolución de incidencia grave		5 horas
ANS_04	Tiempo de resolución de incidencia crítica		2 horas

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.

La licencia de uso tendrá asociado un soporte funcional y técnico para el correcto funcionamiento de la plataforma, monitorización y caza de amenazas y, de forma excepcional, respuesta a incidentes.

Este soporte en función de su naturaleza podrá ser prestado de forma deslocalizada o in-situ:

- **Soporte deslocalizado:** soporte que el adjudicatario (contratista y/o fabricante) deberá prestar de manera deslocalizada desde su centro de seguridad propio.
- **Soporte in-situ:** servicios que el adjudicatario (contratista y/o fabricante) deberá prestar in situ en sedes del Organismo en situaciones excepcionales para la resolución de incidentes de impacto cuando así lo requiera el Organismo.

Las tareas propias a desarrollar por el soporte serán las siguientes:

- Una vez finalizada la fase de despliegue, podrán realizar el alta de nuevos agentes, asesoramiento al Organismo en la resolución de dudas, redespliegue de agentes (en colaboración con los equipos de administración de sistemas del Organismo) o preparación de paquetes de instalación.
- Elaboración de los procedimientos manuales de instalación y configuración del agente para aquellos equipos que no se pueda automatizar su instalación.
- Coordinación, asesoramiento y resolución de incidencias a los equipos de administración de sistemas y otros departamentos del Organismo.
- Gestión y ajuste de la plataforma: gestión de usuarios y permisos, y ajuste fino, entre otras.
- Configuración y despliegue de políticas de detección y respuesta automática.
- Monitorización de la plataforma y atención a las detecciones y alertas, ejecución de acciones de respuesta si fuera necesario y gestión de los incidentes en la plataforma.
- Comunicación con los equipos de contacto del Organismo para notificación y escalado de incidentes según los procedimientos que se establezcan.
- Coordinación, asesoramiento y resolución de incidencias a los distintos departamentos del Organismo, con motivo de mal funcionamiento o denegación del servicio del agente o consola.
- Mantenimiento de la plataforma y los agentes: actualizaciones, aseguramiento de la disponibilidad, solución de incidencias.
- Interlocución con el servicio de soporte y mantenimiento del fabricante.

- Monitorización de la disponibilidad del servicio.
- Seguimiento y corrección de los posibles falsos positivos que se produzcan, mediante generación de excepciones.
- Diseño de cuadros de mandos y reporte periódico de situación.
- Definición y documentación, alineadas con los procedimientos del Organismo, y transferencia de conocimiento sobre casos de uso en esta área, incluyendo runbooks/playbooks para la detección y respuesta.
- Identificación y propuesta de mejoras del servicio y de la funcionalidad de la plataforma.
- En general, atención de consultas técnicas.
- En situaciones excepcionales ante incidentes de gran impacto y a petición del Organismo:
 - Desplazamiento a la sede en la que se haya producido el incidente. Apoyo y colaboración, con los departamentos del Organismo, en la planificación de las medidas de respuesta.
 - Identificación de las causas del incidente.
 - Asesoramiento en la contención de la amenaza y en la recuperación y restauración del servicio.
 - Documentación de las actuaciones realizadas (informe preliminar, informe técnico, informe ejecutivo) y transferencia de conocimiento.

Con periodicidad mensual se entregará por parte del contratista un informe de actividad donde se pormenoricen con detalle las actividades llevadas a cabo, respecto del listado de tareas antes enumerado.

En el apartado Acuerdos de Nivel de Servicio se establecen los umbrales mínimos requeridos para considerar que el servicio se presta a satisfacción.

ANEXO VIII 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, alternatively, **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, alternatively, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a de de

Firmado electrónicamente

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

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

Efectúa las siguientes **DECLARACIONES**

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

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

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

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

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

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

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

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

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

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).

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

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

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

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

....., XX de de 202X

Fdo.

Cargo:

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

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 financiados, estableciéndose las siguientes **obligaciones**:

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

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

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

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

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

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

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

1. 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).

2. 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.

3. 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.

4. PROHIBICIÓN DE DOBLE FINANCIACIÓN

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

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

1. RÉGIMEN JURÍDICO APLICABLE

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

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

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

El contrato se enmarca en el **Componente C11. Inversión I3**

Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y las Entidades Locales

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



Etiquetado verde	Etiquetado digital
No aplica	No aplica

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

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

No aplica.

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

No aplica.

- 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.

No aplica.

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

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.

() Por incumplimiento.

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

() Otras penalidades

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

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

Por ello, en base a lo establecido en el artículo 7 de la Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia, en caso de que no existan datos de titularidad real en las bases de datos de la AEAT de **un participante en el procedimiento de contratación**, el órgano de contratación solicitará a éste la información de su titularidad real.

Esta información deberá aportarse al órgano de contratación en el plazo de cinco días hábiles desde que se formule la solicitud de información. La falta de entrega de dicha información en el plazo señalado será motivo de **exclusión** del procedimiento.

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

- NIF del contratista y, en su caso de los subcontratistas.
- Nombre o Razón Social
- Domicilio fiscal del contratista y, en su caso, subcontratistas
- 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)
- 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)



Dirección General
de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN



Financiado por
la Unión Europea
NextGenerationEU

- 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).