

Este documento se ha obtenido directamente del original, que contenía todas las firmas auténticas, y se han ocultado los datos personales y los códigos que permitían acceder al original.

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

(Expediente nº 2022/48)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

**SUMINISTRO DE SUSCRIPCIONES DE LICENCIAS DE UNA
HERRAMIENTA DE GESTIÓN CENTRALIZADA DE POLITICAS
DE SEGURIDAD PARA LA DIRECCIÓN GENERAL DE SALUD
DIGITAL CON CARGO AL PLAN DE RECUPERACIÓN
TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE
ESPAÑA - FINANCIADO POR LA UNIÓN EUROPEA –
NEXTGENERATIONEU (C11.I03.P14.S13)**

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 DESTINARIO, ORGANO DE CONTRATACIÓN, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO	4
2.	LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO	4
2.1.	Lote, título y objeto	4
2.2.	Características principales de las prestaciones	4
2.3.	Tratamiento de datos de carácter personal por parte del adjudicatario	5
2.4.	Categorización conforme al Esquema Nacional de Seguridad (ENS)	6
2.5.	Tratamientos de datos personales para los programas en modalidad de nube	6
3.	DURACIÓN DEL CONTRATO	7
3.1.	Fecha de inicio de la ejecución	7
3.2.	Plazo de entrega de las licencias	7
3.3.	Plazo de ejecución del contrato	7
3.4.	Prórroga del contrato específico	8
4.	VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN	8
4.1.	Presupuesto de licitación y aplicaciones presupuestarias	8
4.2.	Determinación del precio del contrato	9
4.3.	Tramitación del expediente (a efectos presupuestarios)	12
4.4.	Modificación del contrato específico	13
4.5.	Valor estimado	13
4.6.	Contrato financiado con cargo al presupuesto de la Unión Europea	14
5.	LUGAR Y CONDICIONES DE LA ENTREGA	14
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN	14
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	15
7.1.	Ponderación de los criterios de adjudicación	15
7.2.	Fórmula aplicable al criterio precio	15
7.3.	Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio	16
7.3.1.	Criterios evaluables automáticamente mediante fórmulas	16
7.3.2.	Fórmulas para la evaluación automática de los criterios	16
7.4.	Criterios cuya cuantificación depende de un juicio de valor	17
8.	OFERTAS ANORMALMENTE BAJAS	17
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA	18
9.1.	Obligaciones generales	18
9.2.	Otras condiciones de ejecución del contrato	18
9.3.	Obligaciones de seguridad en cumplimiento del ens	19
9.4.	Obligaciones relativas al cumplimiento de las condiciones de los programas ofertados en modalidad de nube cuando exista tratamiento de datos personales	19
10.	PAGO Y FACTURACIÓN	20

10.1.	Pago del precio	20
10.2.	Condiciones de presentación de las facturas.....	21
11.	GARANTÍA DE LOS BIENES	22
12.	PENALIDADES	22
12.1.	Penalidades fijadas en el sistema dinámico de adquisición.....	22
12.2.	Fórmula para la aplicación de penalidades.....	23
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	23
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS	23
	ANEXO I PRESCRIPCIONES TÉCNICAS.....	26
I.1.	Requisitos funcionales de los programas a suministrar.....	26
	funcionalidades EXIGIDAS	30
I.2.	Requisitos no funcionales de los programas a suministrar.....	35
I.3.	Periodo de vigencia y modalidad de licenciamiento.....	35
I.4.	Requisitos de seguridad de los programas en la nube.....	36
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO	37
II.1.	Servicios de instalación avanzada de los programas a suministrar	37
II.2.	Servicios de soporte de los programas a suministrar	38
	ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS	39
III.1.	Tratamientos de datos y finalidad de los tratamientos	39
III.2.	Medidas técnicas y organizativas	39
	ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE .	40
	ANEXO V MODELO DE DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	41
	ANEXO VI Manifestación de conformidad del responsable del tratamiento DE LOS DATOS DEL ORGANISMO DESTINATARIO43	
	ANEXO VII ENTREGAS PARCIALES	44
	ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO	45
	ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN	46
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	47
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea	47
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR	49

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

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/ Embajadores 181, 28029 - Madrid

Correo electrónico: og.sis@salud.madrid.org

Teléfono:

Órgano de Contratación:

- Comunidad de Madrid. Consejería de Digitalización

2. LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO

2.1. LOTE, TÍTULO Y OBJETO

Lote objeto de licitación: Lote 4 - Software de ciberseguridad

Título del contrato: SUMINISTRO DE SUSCRIPCIONES DE LICENCIAS DE UNA HERRAMIENTA DE GESTIÓN CENTRALIZADA DE POLÍTICAS DE SEGURIDAD PARA LA DIRECCIÓN GENERAL DE SALUD DIGITAL CON CARGO AL PLAN DE RECUPERACIÓN TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA - FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU (C11.I03.P14.S13)

Objeto del contrato:

El objeto de esta contratación es el suministro de licencias de una herramienta para la gestión centralizada de políticas de seguridad de red, la automatización del ciclo de vida de cambios, la gestión de la conectividad de aplicaciones y el aseguramiento del cumplimiento normativo, capaz de operar en entornos híbridos (on-premise y nube), multivendor y multi-cloud, garantizando la trazabilidad y la reducción del riesgo operativo.

2.2. CARACTERÍSTICAS PRINCIPALES DE LAS PRESTACIONES

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

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

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

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

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

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

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

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

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

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

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

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

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

- Sistema : categoría Elija un elemento.
- Sistema : categoría Elija un elemento.
-

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:

.

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

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

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

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

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

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

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

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

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

3. DURACIÓN DEL CONTRATO

3.1. FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

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

3.2. PLAZO DE ENTREGA DE LAS LICENCIAS

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

3.3. PLAZO DE EJECUCIÓN DEL CONTRATO

- ☐ Se requiere la instalación y configuración básica de las licencias, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo⁴ de 30 días hábiles, incluido el plazo de entrega de las licencias.
- ☒ 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: 35 días
- ☐ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario, descritos en el **Anexo II**, apartado 2:

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.

- 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 (€)
221.816,91 €	46.581,55 €	268.398,46 €

El contrato se financia con el Plan de Recuperación, Transformación y Resiliencia, dentro del Componente 11, Inversión 03, Proyecto 14 Subproyecto 13

El importe financiado es de **221.816,91 €**. La Comunidad de Madrid aporta la parte correspondiente al IVA (**46.581,55 €**)

Código de referencia único del proyecto: C11.I03.P14.S13

Fondo MRR 2022/00060

Código de Referencia del Proyecto: 2023/000690

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)	198.635,14 €	41.713,38 €	240.348,52 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	23.181,77 €	4.868,17 €	28.049,94 €

Servicio de soporte, a prestar por el adjudicatario			
TOTAL	221.816,91 €	46.581,55 €	268.398,46 €

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

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

Las obligaciones económicas que se deriven para la Administración por el cumplimiento del contrato serán financiadas por el Presupuesto de Gastos del organismo COMUNIDAD DE MADRID, Centro de Gestión DIRECCIÓN GENERAL DE SALUD DIGITAL, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	Anualidad 2026	Total, IVA incluido
G/928N/64001 (Software)	240.348,52 €	240.348,52 €
G/928N/22703 (Servicios)	28.049,94 €	28.049,94 €

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	20.698,01 €
Resto costes directos	177.352,80 €
Costes indirectos	
Gastos generales 6 %	11.883,05 €
Beneficio industrial 6 %	11.883,05 €

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 calculado como un tanto por ciento (6%) de la suma de los costes directos y el beneficio industrial se ha calculado como un tanto por ciento (6%) de la suma de los costes directos y de los costes indirectos.

Aplicando el 6 % de los gastos generales + 6 % del beneficio industrial a cada concepto los importes resultantes son los siguientes:

Desglose Precio	
Costes directos	
Personal	23.181,77 €
Resto costes directos	198.635,14 €
Total, sin IVA	221.816,91 €

Para el cálculo del precio correspondiente a los servicios a prestar por el adjudicatario, para calcular el valor estimado, se han tenido en cuenta los costes derivados de la aplicación de las normativas laborales vigentes, considerado los costes de personal que deberán encargarse de ejecutar la prestación.

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

Costes de personal							
Perfiles	Dedicación	Salario Base	Especialización tecnológica (120%)	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 32,15%
1 CONSULTOR SENIOR (RESPONSABLE DEL SERVICIO) Consultoría desarrollo y sistemas (AREA 3 Grupo A Nivel 1)	12%	30.904,37 €	37.085,24 €	67.989,61 €	8.158,75 €	8.158,75 €	10.781,79 €
1 técnico de Implantación (AREA 3 Grupo C Nivel 1)	12%	28.423,34 €	34.108,01 €	62.531,35 €	7.503,76 €	7.503,76 €	9.916,22 €

- **Especialización técnica (120 %)**

1. Necesidad de especialización técnica avanzada

Aunque se aplica el Convenio Sectorial, la implantación y operación de herramientas de gestión centralizada de políticas de seguridad requiere un nivel de cualificación significativamente superior al estándar.

Estos sistemas implican:

- Control unificado de políticas de seguridad en infraestructuras complejas.
- Automatización de flujos de cambio en firewalls, routers y dispositivos de seguridad.
- Gestión de riesgos y cumplimiento (compliance) con ENS, ISO 27001, GDPR y normativa sectorial sanitaria.
- Integración con CMDB, directorio corporativo, herramientas ITSM y orquestadores.
- Modelado y automatización de workflows de cambio
- Análisis de reglas, políticas y zonas de seguridad en infraestructura multivendor
- Evaluación automática de riesgos y conflictos en políticas.

Por ello:

Perfil Consultor Senior: Debe poseer experiencia demostrable en proyectos de implantación de herramientas de gestión de políticas de seguridad y automatización de cambios, siendo capaz de:

- Definir y parametrizar flujos de aprobación.
- Modelar políticas y zonas de red.
- Establecer controles automáticos de cumplimiento.
- Asesorar en la optimización y consolidación de reglas de seguridad.

Perfil Técnico de Implantación: Debe contar con experiencia práctica en:

- Integración de la herramienta con dispositivos reales.
- Recolección de políticas, análisis de topología y normalización de reglas.
- Configuración de conectores, APIs y agentes.
- Alineación de la solución con el modelo de red de la organización

2. Exigencias de calidad y plazos establecidas por la DGSD

La DGSD marca parámetros estrictos en cuanto a:

- Disponibilidad del servicio.
- Continuidad operativa durante cambios.
- Estandarización de flujos y procedimientos.
- Visibilidad y trazabilidad completa de cambios y políticas.

Para cumplir con estas exigencias, los perfiles deben ser capaces de:

- Ejecutar configuraciones y migraciones sin impacto.
- Gestionar flujos automatizados de cambio extremo a extremo.
- Correlacionar incidencias con políticas de seguridad.
- Generar auditorías de cumplimiento alineadas con ENS y normativa sanitaria.
- Coordinarse con equipos de comunicaciones, seguridad y sistemas.

La implantación de una herramienta como la solicitada en este documento es un servicio altamente especializado que requiere:

- Conocimientos avanzados en gestión de políticas de seguridad.
- Experiencia real con dispositivos y topologías complejas.
- Capacidad para modelar procesos automatizados alineados con la organización.
- Cumplimiento de normativa estricta del ámbito sanitario.

Por todo ello, el nivel de especialización técnica del 120 % aplicado a los perfiles de Consultor Senior y Técnico de Implantación está plenamente justificado

- Costes de Seguridad Social

Los costes de la Seguridad Social a cargo de la empresa se han estimado en un 32,15 % del coste bruto de personal, incluyendo las cotizaciones por contingencias comunes, desempleo, formación profesional FOGASA, accidentes de trabajo y MEI. Este porcentaje se basa en los tipos de cotización vigentes según la normativa española de Seguridad Social para contratos indefinidos a jornada completa

Los costes de la Seguridad Social a cargo de la empresa se han calculados según el tipo correspondiente al ejercicio 2026, incluyendo las cotizaciones por contingencias comunes, desempleo, formación profesional, FOGASA, mecanismo de equidad intergeneracional y accidentes de trabajo.

Este porcentaje se basa en los tipos de cotización vigentes según la normativa española de Seguridad Social para contratos indefinidos a jornada completa.

CONCEPTO	% APROXIMADO SOBRE BASE DE COTIZACIÓN
Contingencias comunes	23,60 %
Desempleo	5,50 %
Formación profesional	0,60 %
Fondo de Garantía Salarial (FOGASA)	0,20 %
Accidentes de trabajo y enfermedades profesionales	1,50 %
Mecanismo de equidad intergeneracional (MEI)	0,75 %
TOTAL	32,15 %

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.

4.5. VALOR ESTIMADO

Conforme a lo previsto en el artículo 101.5 de la LCSP el valor estimado asciende a **221.816,91 € euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	221.816,91 €
Importe máximo por modificación prevista, sin IVA	
TOTAL	221.816,91 €

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

☒ **SI está sujeto a regulación armonizada**

☐ **NO está sujeto a regulación armonizada**

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

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

☐ No.

☒ Sí. Instrumento /Fondo/Programa/Mecanismo: Plan de Recuperación, Transformación y Resiliencia / Plan de Atención Digital Personalizada / Componente 11 Inversión 3.

Código de operación/Proyecto/Iniciativa: Asistencia digital Personalizada

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: Centro de Datos Administración y Soporte (CEDAS)
- Correo electrónico: direccion.cedas@salud.madrid.org
- Teléfono: 626661756 / 615043824
- 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 VII**.

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

6. INCOMPATIBILIDADES PARA LA LICITACIÓN

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

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

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

☐ Otras:

NO APLICA

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

NO APLICA

7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN⁶

7.1. PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN

☐ El único criterio de adjudicación es el precio

☒ Solo se utiliza el precio y otros criterios evaluables mediante fórmulas, con los siguientes pesos:

SOBRE 1.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 1.2. Precio
10 PUNTOS	90 PUNTOS

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

SOBRE 1. Criterios que dependen de un juicio de valor	SOBRE 2.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 2.2. Precio
NO APLICA.	NO APLICA.	100 PUNTOS

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)

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

O_{b_i} es el precio más bajo ofertado (IVA excluido)

O_{t_i} es el presupuesto máximo de licitación (IVA excluido)

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

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

Donde:

C_i es la puntuación en base al criterio precio, asignada a la oferta del licitador i

P , es la ponderación del criterio precio, la cual deberá ser como mínimo de 40 puntos sobre 100.

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

O_{min} es el precio más bajo ofertado (IVA excluido)

O_{max} es el precio de la oferta más alta (IVA excluido)

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

7.3.1. CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS

Se valorará las propuestas que presenten mayores capacidades de licenciamiento del paquete en la unidad de medida (**Firewall Units**) de la herramienta de gestión de políticas de seguridad en las mismas condiciones que se definen en este documento de licitación en base a los siguientes criterios.

CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓN, según apartado 7.3.2.
Inclusión sin coste adicional en la propuesta de 5 Firewall Units adicionales	5	Sí/No
Inclusión sin coste adicional en la propuesta de 10 Firewall Units adicionales	10	Sí/No

Solo se puede marcar como SI una o ninguna de las dos opciones, pero en ningún caso las dos.

7.3.2. FÓRMULAS PARA LA EVALUACIÓN AUTOMÁTICA DE LOS CRITERIOS

Función Maximizar:

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

Donde:

- C_i es la puntuación en base al criterio C , asignada a la oferta del licitador i ;
- P es la ponderación del criterio C ;
- X_i es el valor ofertado por el licitador i en el criterio C ;

- X_{\max} es el valor máximo ofertado por los licitadores en el criterio C o el umbral de saciedad si éste fuese inferior y se hubiese definido.

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

Función Minimizar:

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

Donde:

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

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

Función Sí/No (maximizar binario):

$$X_i = P$$

Donde:

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

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

NO APLICA

8. OFERTAS ANORMALMENTE BAJAS

Se apreciará que la oferta es anormalmente baja cuando se produzcan las siguientes condiciones de forma concurrente:

- Si existiendo 4 o más licitadores las ofertas económicas presentadas resultan inferiores en más de 20 unidades porcentuales a la media aritmética de las ofertas presentadas. No obstante, si entre ellas existen ofertas que sean superiores a dicha media en más de 20 unidades porcentuales, se procederá al cálculo de una nueva media sólo con las ofertas que no se encuentren en el supuesto indicado. En todo caso, si el número de las restantes ofertas es inferior a tres, la nueva media se calculará sobre las tres ofertas de menor cuantía. Si, por el contrario, han concurrido menos de cuatro licitadores, resultarán de aplicación las previsiones del artículo 85 apartados 1 a 3 del Reglamento 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas.
- A la condición anterior, siempre que existan criterios diferentes al precio, se deberá añadir la siguiente para apreciar el carácter anormal o desproporcionado de las ofertas.

- ☐ Cuando la puntuación en el criterio de calidad de mayor peso de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media de los valores ofertados: *indicar % o importe*.
- ☒ Cuando la puntuación conjunta de todos los criterios de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media la puntuación de todas las ofertas en estos criterios: 0,01%.

9. CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA

9.1. OBLIGACIONES GENERALES

Al presente contrato le resultan de aplicación las siguientes obligaciones, conforme a lo establecido en los pliegos reguladores del sistema dinámico de adquisición:

- a) A ofertar únicamente programas con distribución comercial, no pudiendo aplicar precios superiores a los de mercado conforme a las condiciones del apartado 17.2 c) del PCAP, y que satisfagan las prestaciones de la garantía obligatoria del fabricante previstas en el apartado III.6 del PPT.
- b) La obligación de cumplimiento de la condición especial de ejecución relativa a la disponibilidad de los planes de formación conforme al apartado 27.5.6 apartado 1 del PCAP y, en su caso, las condiciones de ejecución previstas en el apartado 9.3 de este documento de invitación.
- c) Las obligaciones referidas a la protección de datos personales, en los términos previstos en la cláusula 27.5.6 apartado 2 del PCAP.
- d) La obligación de confidencialidad del apartado 27.5.8 del PCAP.
- e) Las obligaciones establecidas en el apartado 27.5.9 del PCAP respecto al personal laboral.
- f) A facilitar la información técnica prevista en los apartados III.9 y III.10 del PPT de los productos ofertados, en caso de resultar adjudicatario.
- g) Las obligaciones de comunicación de la subcontratación y la acreditación de los pagos a los subcontratistas conforme al apartado 27.11 del PCAP. En su caso, y conforme a lo previsto en el artículo 215.2.e) de la LCSP, el contratista principal no podrá subcontratar las siguientes tareas críticas:

NO APLICA
- h) Si el contrato incluye servicios a prestar por el adjudicatario, estará obligado al cumplimiento de las condiciones salariales de los trabajadores conforme al convenio colectivo sectorial de aplicación conforme al artículo 122.2 de la LCSP.
- i) El adjudicatario nombrará un Coordinador Técnico del Contrato que actuará como interlocutor único a todos los efectos frente a la entidad destinataria del contrato, canalizando las comunicaciones y responsabilizándose de la gestión de la prestación por parte de la empresa adjudicataria.

9.2. OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO

NO APLICA

9.3. OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

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

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

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

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

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

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

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

nube establecido en la UE/EEE ofrezca garantías adecuadas conforme a lo previsto en el Capítulo V del RGPD⁷.

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

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

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

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

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

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

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:

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

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 (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: Comunidad de Madrid. Consejería de Digitalización - A13002908
- Órgano responsable del contrato específico: Dirección General de Salud Digital - GE0021859
- Órgano gestor: Comunidad de Madrid. Consejería de Digitalización - A13002908
- Unidad tramitadora: UGEP SALUD DIGITAL: GE0021859

- Órgano administrativo con competencias en materia de contabilidad pública: 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>: Será el número del contrato específico (xxxx/aaaa) o, en su defecto, el número que para esta tramitación asigne el organismo destinatario.

11. GARANTÍA DE LOS BIENES

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

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

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

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

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

12. PENALIDADES

12.1. PENALIDADES FIJADAS EN EL SISTEMA DINÁMICO DE ADQUISICIÓN

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

	Valor fijado en el SDA	Valor fijado en el contrato específico	Fórmula de cálculo
Incumplimiento de las condiciones especiales de ejecución, excepto las relativas a subcontratación.	2% de la facturación del periodo	NO APLICA	Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo	NO APLICA	Según ANS.

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

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

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

La oferta 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:
 - Documentación técnica que acredite el Cumplimiento de requisitos ANEXO I y ANEXO II
 - El licitador deberá en este documento indicando no solo el cumplimiento del requisito SI o NO, sino que se deberá complementar con observaciones y hacer un detalle más completo en la respuesta.
 - La DGSD se reserva la capacidad de solicitar la comprobación por los medios técnicos que estime el cumplimiento de ciertos requisitos antes de la adjudicación definitiva. En el caso de que no se cumplan tal y como está indicado en pliego de requisitos técnicos, o como haya matizado el licitante en su respuesta, se considerará como nula toda la propuesta, siendo motivo suficiente para su no aceptación. Por este motivo, se solicita que en la oferta técnica a presentar se incluya el máximo nivel de detalle en el cumplimiento de los requisitos planteados, para evitar el máximo posible dudas sobre la respuesta.

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://gestiona5.madrid.org:8203/sap/bc/webdynpro/sap/zfrms_wd_le_003# 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.

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.

- No se tendrán en consideración las respuestas que no demuestren suficientemente el cumplimiento de TODOS los requisitos solicitados en este documento.
- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - Documentación técnica que acredite el Cumplimiento de requisitos ANEXO II
- 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.

- NO APLICA

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

EN LO QUE ESTE DOCUMENTO DE INVITACIÓN SE OPONGA A LOS PLIEGOS DEL SISTEMA DINÁMICO DE ADQUISICIÓN, PREVALECEÁN ESTOS ÚLTIMOS.

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

EL TITULAR DEL ÓRGANO DESTINATARIO (CARGO): Directora General de Salud Digital

Firmado digitalmente por: NURIA RUIZ HOMBREBUENO
Fecha: 2026.02.17 10:06

Firmado electrónicamente (nombre y apellidos): Nuria Ruiz Hombrebueno

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

Según se dispone en el Decreto 76/2023, de 5 de julio, del Consejo de Gobierno, por el que se establece la estructura orgánica básica de las Consejerías de la Comunidad de Madrid, y según Decreto 261/2023, de 29 de noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Digitalización, corresponde a la Dirección General de Salud Digital (DGSD): “La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Servicio Madrileño de Salud, de acuerdo con las necesidades explicitadas por este último, así como la tramitación electrónica en el Servicio Madrileño de Salud” y “La provisión y gestión de los servicios y equipamientos informáticos sanitarios del Servicio Madrileño de Salud, en colaboración con el Servicio Madrileño de Salud”

De acuerdo con dichas competencias, la DGSD, desde los Centros de Procesos de Datos (CPD) principales y el CPD de respaldo externalizado en Tres Cantos, proporciona servicios TIC sanitarios a más de 6.800.000 ciudadanos y cerca de 90.000 profesionales de la red sanitaria pública de la Comunidad de Madrid.

Por tanto, en los CPD centrales del SERMAS gestionados por la DGSD se despliegan todas las aplicaciones y servicios TI de su competencia encargados de albergar los SS. II., que sustentan la operativa de gran parte de las funcionalidades del Sistema Sanitario Público.

Estos CPD soportan la totalidad de los Sistemas de Información (SS.II.) corporativos, que garantizan la operativa diaria del sistema sanitario público. Actualmente se alojan más de 2.500 aplicaciones críticas, entre las que se encuentran:

- La Historia Clínica Electrónica:
 - Atención Primaria: APMADRID
 - Atención Hospitalaria: HCIS, SELENE
- Sistemas de medicamentos: Receta Electrónica, RUV
- Banco de Sangre
- Aplicaciones de emergencias del SUMMA 112
- Aplicaciones hospitalarias departamentales (Laboratorio, Farmacia, UCI, Dietética, Urgencias/Triaje, etc.)

La pérdida de servicio o de funcionalidad de cualquiera de estos sistemas constituye un riesgo crítico para la continuidad asistencial y podría comprometer directamente la seguridad del paciente. Por tanto, la infraestructura tecnológica que los soporta debe contar con los máximos niveles de resiliencia, control, seguridad, automatización y supervisión.

Además de que dichos sistemas TI sanitarios tienen grados de criticidad muy altos en lo funcional, existe la obligación legal de dar respuesta a aspectos de privacidad, confidencialidad y seguridad tanto en el acceso como en la custodia y almacenamiento de la información sanitaria. En este sentido, es importante tener en consideración la obligación del cumplimiento de la actual normativa tanto europea (Reglamento General de Protección de Datos - RGPD) como nacional (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales - LOPD-GDD). También, por ser el SERMAS una AAPP, es obligado el cumplimiento del Esquema Nacional de Seguridad (ENS) que, como es lógico, obliga a tratar los datos personales sanitarios de los ciudadanos con los más altos niveles exigidos de seguridad para datos personales.

Los sistemas que conforman el ecosistema TIC sanitario deben, por tanto:

- Mantener una gestión estricta de accesos y comunicaciones.
- Garantizar la segmentación de red, la protección perimetral y la correcta aplicación de políticas de seguridad.
- Asegurar el cumplimiento normativo continuo (auditorías, trazabilidad, control de reglas).
- Evitar la existencia de reglas inseguras, duplicadas, obsoletas o inconsistentes, que puedan comprometer la disponibilidad o confidencialidad de datos

Dado el volumen, criticidad y estrictas obligaciones legales de los sistemas de información del SERMAS, la DGSD considera imprescindible el disponer de una herramienta de gestión integral de políticas de seguridad de red, automatización de cambios, auditoría continua, segmentación avanzada y gestión de conectividad de aplicaciones, que garantice la seguridad, disponibilidad y cumplimiento normativo en los CPD de la Red Sanitaria Pública.

Dicha herramienta tendrá las siguientes capacidades:

1. **Gestionar de forma centralizada políticas de red en un entorno heterogéneo:** Incluyendo firewalls de múltiples fabricantes, redes híbridas, SDN, cloud público/privado y redes hospitalarias distribuidas.
2. **Automatizar los cambios de red**, eliminando errores humanos Con tiempos de aplicación de cambios reducidos de días a minutos y con validaciones automáticas que eviten brechas.
3. **Garantizar el cumplimiento normativo** continuo (ENS, RGPD y estándares sectoriales. Gracias a auditoría permanente, verificación de reglas, reporting y trazabilidad completa.
4. **Gobierno, control y auditoría de entornos de microsegmentación** y modelos Zero-Trust, asegurando su correcta definición, coherencia y cumplimiento mediante políticas centralizadas
5. **Gestionar la conectividad de aplicaciones críticas**, Mapeando dependencias, flujos, puertos, protocolos y accesos necesarios para más de 2.500 aplicaciones sanitarias.

6. Integrarse con infraestructuras complejas y multivendor, para que los CPD centrales operen de manera eficiente, automatizada e interoperable.

7. Aprovechar capacidades avanzadas de análisis, correlación inteligente de políticas y detección proactiva de riesgos, que permitan anticipar impactos y desviaciones de seguridad antes de su aplicación en entornos productivos.

8. Gobierno de políticas basado en topología real.

La solución deberá mantener un modelo dinámico y actualizado de la topología real de red, incluyendo enrutamiento, zonas de seguridad y dependencias entre dispositivos, permitiendo validar políticas y cambios en función del camino efectivo del tráfico y no únicamente de configuraciones aisladas.

9. Matriz de Accesos viva y vinculada a cambios.

La matriz de acceso corporativa deberá estar directamente vinculada a los flujos de cambio, de forma que cualquier modificación propuesta o aplicada sea validada automáticamente contra dicha matriz, generando alertas, bloqueos o evidencias de excepción debidamente justificadas.

11. Gestion del ciclo de vida completo de la regla.

La solución deberá cubrir el ciclo de vida completo de las reglas de seguridad, incluyendo solicitud, diseño, aprobación, implementación, verificación post-cambio, uso efectivo, recertificación periódica y retirada controlada con como mínimo:

- Solicitud
- Diseño de la regla óptima
- Simulación (what-if)
- Aprobación
- Implementación
- Verificación post-cambio
- Medición de uso real
- Recertificación
- Retirada controlada

12. Optimización basada en uso REAL + riesgo.

La optimización de reglas y objetos deberá basarse tanto en el tráfico real observado como en el análisis de riesgo y cumplimiento, evitando recomendaciones puramente técnicas sin contexto de seguridad o negocio.

13. Separación clara entre diseño y ejecución.

La solución deberá desacoplar el diseño y validación de políticas de su ejecución técnica, permitiendo validar cambios independientemente del acceso directo a los dispositivos productivos.

Por tanto, los objetivos de adquisición de esta herramienta plantean la mejora de los principales aspectos:

1. **Posibilitar la implementación de la política de acceso a la red** definida en la Política de Seguridad Corporativa en forma de Matriz, de tal forma que pueda ser contrastada contra el conjunto de reglas activo en el total de los elementos de red configurados. La matriz se entiende como una matriz de redes, en el que, para cada combinación de tráfico entre redes, se establece que tráficos están permitidos, de tal forma que se pueda impedir o alertar de a cualquier cambio que viole lo establecido en dicha matriz que representa la Política de Acceso corporativa. Se trata, en definitiva, de disponer de un proceso de auditoria continua sobre los cambios en los accesos que se intenten implementar.
2. **Mantener un control centralizado de las configuraciones** y sus diferentes versiones del equipamiento “core” en el que se configuran las reglas de control de acceso a la red de datos y el enrutamiento, de cara a poder analizar los cambios y participar en el ciclo de vida de su implementación (aprobación, programación, vuelta atrás en caso de fallo...)
3. **Posibilitar la implementación de un flujo de aprobación de los cambios** de tal forma que se asegure la puesta en marcha de las modificaciones a las reglas de control de acceso sobre la red corporativa, en base a los procedimientos que se definan en la Política de Seguridad Corporativa.
4. **Detectar cambios que no requieran de una configuración adicional a la ya existente.** Esto permite depurar las configuraciones en los equipos a las mínimas necesarias y liberar de trabajo adicional a los administradores de los sistemas al filtrar este tipo de solicitudes.
5. **Posibilitar la optimización de reglas necesarias**, así como los objetos configurados en el equipamiento en base al tráfico real detectado y a las reglas y objetos que por tantos son realmente utilizados. El objeto de disponer de una configuración optimizada minimiza el riesgo de fallos en la implementación de la política de seguridad, así como la visibilidad y transparencia de esta.
6. **Permitir la generación automática de la topología de red** y representar el modelo de enrutamiento con el diferente equipamiento de nivel 3 efectos de poder determinar, dado un origen y un destino, el camino por el que fluye el tráfico y el grado de acceso de dicho tráfico en función de los elementos que atraviesa (routers, balanceadores y firewalls) y las reglas de acceso que se encuentran implementadas en ellos.
7. **Permitir la generación de casos “what-if”** que permitan analizar impactos en la política de acceso de la red de datos sin necesidad de llevarlos al entorno productivo.

La herramienta deberá permitir la simulación de escenarios “what-if” considerando múltiples dispositivos, saltos intermedios y tecnologías heterogéneas, evaluando impactos combinados en seguridad, cumplimiento y conectividad extremo a extremo.

FUNCIONALIDADES EXIGIDAS

La herramienta permite para la gestión unificada de firewalls y dispositivos de red que permitiendo supervisar y analizar las políticas de seguridad relacionadas con los firewalls de múltiples proveedores, optimizar y volver a certificar las reglas de los firewalls y hacer un seguimiento de los cambios en la red para garantizar un cumplimiento normativo permanente.

La herramienta incorpora las siguientes funcionalidades al respecto

Tipos de Despliegue

- La solución ofrece una arquitectura escalable con opciones de despliegue en alta disponibilidad, tanto para entornos on-premise (Nube Privada) como en nube pública.
- La solución ofrece opciones de despliegue que permiten la gestión centralizada de políticas de seguridad, manteniendo al mismo tiempo la autonomía local cuando sea necesario.
- La solución estará fundamentada en arquitecturas nodo simple o multimodo, permitiendo la escalabilidad (Scale-up / Scale-out) y la adaptación a la distribución de los equipos que se monitorizan (arquitectura distribuida) en base a las necesidades de rendimiento y escalabilidad de la DGSD.

Funcionalidades Generales

- La solución proporcionar una gestión integral y automatizada de las políticas de seguridad de red, adaptándose a las necesidades específicas de cada organización y garantizando una postura de seguridad robusta y coherente en entornos de red complejos y heterogéneos.
- Gestión centralizada y unificada de los principales proveedores de firewalls y routers.
- Depuración de reglas: identificación de reglas y objetos que no se utilizan en las configuraciones de firewalls y listas de control de acceso de switches y routers.
- Seguimiento de cambios, alertas e informes.
- Cumplimiento continuo de los estándares, incluidos PCI DSS, NIST, NERC e ISO27001 entre otros.
- Informes de auditoría integrados.
- Información de topología de red para que la configuración de red sea más rápida y precisa.
- Análisis de impacto de riesgo antes de configurar los cambios en las políticas.
- Documentación y recertificación de reglas.
- Visibilidad y control centralizados de los cambios en entornos complejos.
- Ofrece una vista unificada de todas las reglas de seguridad y configuraciones en la infraestructura de red.

- Permite la identificación de configuraciones obsoletas o riesgosas en firewalls y dispositivos de seguridad.
- Proporciona un historial detallado de cambios en las políticas de seguridad, facilitando auditorías y análisis forenses.
- Análisis preciso y eficiente de los cambios de seguridad en la red que reduce los tiempos de inactividad.
- Preparación de auditorías más rápida.
- Se conocen todas las políticas de seguridad de la red y los cambios se ajustan a las políticas corporativas para obtener una gestión efectiva del riesgo.

Gestión del Cumplimiento y Reducción de Riesgos

- Evalúa continuamente las reglas de firewall para garantizar su alineación con normativas como PCI DSS, HIPAA, ISO 27001 y NIST.
- Identifica reglas redundantes, ineficaces o que presentan riesgos innecesarios.
- Automatiza la validación del cumplimiento mediante reportes personalizables.
- Capacidad de crear una relación jerárquica de zonas.
- Capacidad de definir una política de segmentación de red que permita solo reglas de FW de host a host, de host a subred, de subred a host o de subred a subred para la interacción de zona a zona.

Optimización de Políticas de Seguridad

- Capacidad de generar una matriz de políticas de cumplimiento basada en las políticas de acceso a la red existentes.
- Análisis y recomendación de optimización de reglas para reducir la complejidad y mejorar la eficiencia.
- Elimina configuraciones innecesarias y mejora el rendimiento de los firewalls y otros dispositivos de seguridad.
- Facilita la segmentación de la red mediante la definición de zonas seguras.

Integración con Entornos Híbridos y Multi-Nube

- Soporte para entornos on-premises, híbridos y en la nube.
- Integración con soluciones de seguridad en la nube como AWS, Microsoft Azure y Google Cloud Platform.
- Visibilidad de políticas en entornos SDN y contenedores, garantizando seguridad en arquitecturas modernas.

- La solución debe tener una integración nativa con soluciones IPAM/DDI para mapear subredes almacenadas a segmentos de red para generar violaciones de acceso a red precisas a través de una matriz de conectividad de segmento de red a segmento de red.

Informes

- Capacidad de ver una puntuación de permisividad en las reglas del firewall.
- La solución debe poder buscar todas las reglas que pertenecen a un determinado nombre de propietario que pueden aparecer en varios campos de una regla/metadatos y que son altamente permisivas en una consulta simple.
- La solución debe ser capaz de buscar todas las reglas que son candidatas para el desmantelamiento que no se han enrutado al proceso de desmantelamiento para centrarse en las reglas que aún no se han manejado para el desmantelamiento
- Alertas e informes de incumplimiento.
- Informe de cambios anticipados.
- La solución debería poder presentar reglas para la limpieza a lo largo del tiempo en una visualización de línea de tendencia.

Soporte a Dispositivos y Plataformas

- Ofrece compatibilidad con una amplia gama de firewalls, routers, dispositivos de seguridad y plataformas en la nube, incluyendo:
 - o Firewalls de Próxima Generación (NGFW): Fortinet, Check Point. Palo Alto Networks
 - o Dispositivos de Seguridad de Red: F5 BIG-IP, Blue Coat Proxy, Zscaler.
 - o Routers y Switches: Cisco
 - o Entornos en la Nube: AWS Security Groups, Microsoft Azure Network Security Groups, Google Cloud Firewall.
 - o Plataformas de Virtualización y SDN: VMware NSX, Cisco ACI.

Automatización del ciclo de cambios

Su objetivo principal es automatizar y agilizar el proceso de cambios en las políticas de seguridad, garantizando que cada modificación sea segura, cumpla con las normativas vigentes y se alinee con las políticas internas de la DGSD.

La herramienta incorpora las siguientes funcionalidades al respecto:

- Permite Diseño de cambios automatizado basado en la topología de red y seguridad.

- Análisis proactivo de los impactos de los cambios, simulación de riesgos e impacto de las propuestas de cambio en el cumplimiento normativo; antes y después de la implementación.
- Opción de implementación automática o asistida de cambios en dispositivos de red y seguridad, según las capacidades del fabricante y los controles definidos por la organización pasando por la verificación del cambio, el diseño del cambio, el análisis de los riesgos que este supone y finalmente su implementación.
- Flujos de trabajo personalizados e ilimitados.
- Integración con sistemas existentes: La solución se integra sin problemas con una variedad de sistemas y plataformas que dispone la DGSD, incluyendo entre otros, firewalls de múltiples proveedores (Checkpoint y Fortinet), entornos de nube privada (VMWARE) e híbrida, sistemas de gestión de tickets (ITSM) como CA, Remedy y otras herramientas de seguridad y gestión de redes.
- Debe ser posible establecer un flujo de aprobaciones para que cada cambio pueda descartarse, notificarse y aprobarse. El sistema debe poder definir varias tareas para aprobar únicamente los flujos que le corresponden al aprobador. Por ejemplo, dependiendo del firewall en cuestión, la criticidad del cambio o su urgencia. La configuración debe realizarse mediante la interfaz de usuario.
- La solución debe ser capaz de orquestar procesos de revisión de reglas alineando redes en reglas con propietarios de una fuente de datos externa, orquestar el proceso de revisión de reglas entre los propietarios de la red, habilitar la modificación de reglas para garantizar que las reglas parcialmente certificadas alcancen los criterios de certificación completos y utilizar flujos de trabajo para certificar reglas o deshabilitarlas.
- Permite diseñar y personalizar flujos de trabajo automatizados para gestionar solicitudes de cambio en las políticas de seguridad, desde la solicitud inicial hasta la implementación y verificación final.
- La solución debe ser capaz de definir los procesos de la empresa en un nuevo flujo de trabajo para solicitar flujos. La configuración de flujos de trabajo avanzados debe ser posible mediante la interfaz de usuario. La solución debe ser capaz de tener múltiples flujos de trabajo para diferentes procesos, por ejemplo, para diferentes departamentos. Se requiere soporte preconfigurado y la posibilidad de añadir o eliminar pasos mediante la interfaz de usuario.
- La solución debe ser capaz de soportar un flujo de trabajo totalmente automatizado (automatización sin intervención) con una opción para cambiar el nivel de automatización por paso a través de la interfaz de usuario lista para usar.
- La solución debe ser capaz de orquestar procesos de revisión de reglas alineando redes en reglas con propietarios de una fuente de datos externa, orquestar el proceso de revisión de reglas entre los propietarios de la red, habilitar la modificación de reglas para garantizar que las reglas parcialmente certificadas alcancen los criterios de certificación completos y utilizar flujos de trabajo para certificar reglas o deshabilitarlas.

- Evaluación proactiva de riesgos: Durante el proceso de diseño del cambio, la herramienta evalúa automáticamente las solicitudes en función de las políticas de seguridad corporativas y las normativas de cumplimiento, alertando sobre posibles conflictos o riesgos antes de la implementación.
- Cumplimiento continuo: ayuda a mantener el cumplimiento con normativas como PCI-DSS, NERC-CIP e HIPAA, asegurando que cada cambio en la red esté alineado con los estándares requeridos.
- Análisis de rutas y simulación de tráfico: Ofrece capacidades para analizar rutas de tráfico y simular cambios, lo que facilita la solución de problemas y la planificación de modificaciones en la red sin interrumpir el servicio.
- La solución debe poder simular consultas de análisis de tráfico y solucionar problemas de conectividad de red con integración LDAP (ID de usuario) para evaluar el acceso y la conectividad de los usuarios.
- Capacidad de personalizar el mapa de topología con rutas basadas en políticas para un análisis de ruta preciso.
- La solución debe ser capaz de solucionar problemas de tráfico Norte-Sur o Este-Oeste que pasa por VPC, puertas de enlace de tránsito (TGW), conexión directa (a través de VPC o TGW), VPN, GWLB.
- Capacidad de personalizar el mapa de topología con rutas basadas en políticas para un análisis de ruta preciso.

ALCANCE DEL SUMINISTRO

Suscripciones de licencias de una herramienta de gestión de políticas de seguridad en el modo de licenciamiento que cumpla con todos los requisitos funcionales exigidos en este documento con capacidad para gestionar **30 Firewall Units**.

A efectos de licenciamiento, 1 Firewall Unit equivale a uno de los siguientes elementos:

- 1 firewall físico o virtual individual.
- 1 clúster de firewall físico o virtual en activo/pasivo (active/standby).
- 1 Leaf de Cisco ACI.
- 1 firewall en entornos cloud.
- 4 CPUs en entornos SDN.
- 10 instancias de balanceadores de carga.
- 20 routers/switches.

El suministro incluye el acceso a las funcionalidades del nivel de producto correspondiente y la cobertura durante el periodo de suscripción definido en el punto I.3 de este documento.

La equivalencia debe entenderse en los términos que define el apartado III.1 del Pliego de Prescripciones Técnicas.

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

NO APLICA

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Vigencia de las licencias:

Programa	Periodo de vigencia del licenciamiento
Número de suscripciones indicadas en documento o equivalentes	Tres Años

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

Programa	Derechos durante la vigencia de las licencias				
Programas bajo modalidad de licenciamiento en base a capacidades/funcionalidades y por dispositivo.	<ul style="list-style-type: none">• Derecho de uso: por nivel de licenciamiento en base a capacidades/funcionalidades y por dispositivo.• Derecho de actualización: Actualización de versiones y configuraciones que resulten por el fabricante.<ul style="list-style-type: none">○ Actualización de versiones debido al mantenimiento correctivo, evolutivo, perfectivo y adaptativo del software.○ Acceso a parches, actualizaciones menores y “hot-fixes”.• Derecho Acceso multicanal: telefónico, e-mail, web de soporte.• Derecho de Interacción on-line con técnicos especializados.• Derecho de informes preventivos sobre el estado de la configuración• Derecho de acceso a cuadro de mando con el estado de los productos y su uso.• Derecho de acceso a documentación: a una base de conocimiento para la resolución de problemas.• Derecho de consulta al fabricante (soporte del fabricante):<ul style="list-style-type: none">○ Horario: <i>Standard Support</i>• Derecho de Tratamiento específico para aquellas incidencias con prioridad muy alta.				
	Nivel de gravedad	1: Crítico	2: Alto	3: Medio	4: Bajo
		El sistema de producción está inactivo	Fallo de función o característica principal	Fallo de función o característica menor	Problema menor

	Descripción del nivel de gravedad	El sistema de producción está inactivo. El producto no funciona, por lo que se ha generado una disrupción total de la actividad. No existe solución alternativa temporal disponible.	Fallo de funcionalidad principal. Las operaciones están muy restringidas, aunque la actividad puede continuar, pero de forma limitada. Existe una solución alternativa temporal.	Fallo de funcionalidad menor. El producto no funciona como debiera, por lo que se produce una pérdida de uso menor. Es posible que haya una solución alternativa temporal.	No se ha producido pérdida de servicio. Por ejemplo, puede tratarse de una solicitud de documentación, información general o una solicitud de mejora de Software
	Objetivos de tiempos de respuesta				
	Standard Support	2 horas	8 horas	12 horas	1 día hábil

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

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

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

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

¹⁰ El RD 311/2022 hace referencia, en su medida [op.nub.1.1] a las guías CCN-STIC que sean de aplicación. Se trataría de la guía para el "software como servicio (SaaS)". En el momento actual, al no estar publicada dicha guía, este requisito no es aplicable.

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

I.5. SERVICIOS DE INSTALACIÓN AVANZADA DE LOS PROGRAMAS A SUMINISTRAR

Todos los equipamientos quedarán instalados, configurados y puestos en marcha de acuerdo con el Plan de Proyecto.

El alcance de los trabajos que se definen en este pliego incluye el suministro, instalación, configuración, personalización, integración de los dispositivos principales que estipule la DGSD, traspaso de conocimientos, puesta en servicio y los servicios técnicos necesarios para dicha puesta en marcha, así como las pruebas necesarias para la puesta en producción.

La instalación será realizada por personal técnico certificado en las tecnologías a desplegar

Los servicios de instalación avanzada incluirán:

- Diseño de la implantación de los productos adaptados a los requisitos tecnológicos de la DGSD.
- o La propuesta y documentación de diseño a alto y bajo nivel para los nuevos componentes solicitados.
- Instalación física y lógica, de todos los elementos suministrados, configuración, integraciones con los sistemas existentes y las pruebas necesarias para su puesta en funcionamiento en las instalaciones de la DGSD en base a los requisitos de diseño acordados.
- Traspaso al personal de administración de la DGSD de la configuración y entregas de documentación.
- o Transferencia conocimiento y entrega de documentación de proyecto.

Las ofertas desglosaran el importe correspondiente a la instalación avanzada.

Hito	Descripción del hito y sus entregables	Plazo	Porcentaje de la prestación
HITO_01	<p>Descripción del hito: Diseño de la implantación de los productos adaptados a los requisitos tecnológicos de la DGSD</p> <p>Entregables:</p> <ul style="list-style-type: none"> - Documentos de Diseño Alto nivel y Bajo Nivel 	5 días	15%
HITO_02	<p>Descripción del hito: Instalación física y lógica, de todos los elementos suministrados, configuración, integraciones en dispositivos principales y las pruebas necesarias para su puesta en funcionamiento en las instalaciones del Servicio Madrileño de Salud en base a los requisitos de diseño acordados.</p>	25 días después de la aceptación del HITO_01	70%

	Entregables: <ul style="list-style-type: none"> • Documento de instalación. • Cuaderno de pruebas u otras evidencias de que se han realizado las tareas 		
HITO_03	<p>Descripción del hito: transferencia de conocimiento al personal de administración de la DGSD del despliegue de la solución y situación final de la plataforma.</p> <p>Entregables:</p> <ul style="list-style-type: none"> • Documento de situación final de la plataforma. • Manuales de Administración. 	5 días después de la aceptación del HITO_02	15%

I.6. SERVICIOS DE SOPORTE DE LOS PROGRAMAS A SUMINISTRAR

NO APLICA

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

II.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:
- Categorías de datos personales tratados:
- Datos sensibles tratados (si procede) y restricciones o garantías aplicables:
- Naturaleza del tratamiento:
- Finalidad(es) del tratamiento:
- Duración del tratamiento:

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

II.2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

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

NO APLICA

ANEXO III NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

NO APLICA

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 2
Propuesta de adjudicación/Expediente organismo destinatario	
Objeto:	

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

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

DECLARA

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

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

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

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

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

(Fecha, firma y nombre completo del representante legal)

Fdo. electrónicamente

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

Organismo destinatario:	
AM/SDA:	SDA 25/2022 LOTE 2
Propuesta de adjudicación/Expediente organismo destinatario	
Objeto:	

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

MANIFIESTO

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

Indicar nombre y cargo. Firma electrónica.

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: Haga clic o pulse aquí para escribir texto.

Acuerdos de nivel de servicio:

NO APLICA

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.¹¹
- **Certificación positiva** de la Agencia Estatal de Administración Tributaria de hallarse los subcontratistas al corriente en el cumplimiento de las obligaciones tributarias o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.
- **Certificación positiva** de la Tesorería General de la Seguridad Social de hallarse los subcontratistas al corriente de sus obligaciones con la Seguridad Social o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a de de

Firmado electrónicamente

¹¹ La declaración responsable deberá formularse en los siguientes términos “Que ni el firmante de la declaración, ni la persona física/jurídica a la que representa, ni ninguno de sus administradores o representantes se hallan incursos en supuesto alguno a los que se refiere el artículo 71 de la LCSP.”

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 financiados¹² por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiables, estableciéndose las siguientes **obligaciones**:

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

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

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

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

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

¹² O es susceptible de ser financiado en caso de no haberse aún confirmado la selección por las autoridades correspondientes.

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

5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

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

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

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

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

7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

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

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

8. PROHIBICIÓN DE DOBLE FINANCIACIÓN

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

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

1. RÉGIMEN JURÍDICO APLICABLE

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

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

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

El contrato se enmarca en el **Componente 11. Inversión 03. Plan de Atención Digital Personalizada**

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

Etiquetado verde	Etiquetado digital
0 %	100 %

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

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

No aplica

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

No existen obligaciones específicas.

c) Condiciones que deben cumplir las prestaciones establecidas en la evaluación de los aspectos del principio de DNSH (*Do No Significant Harm*) con relación los seis objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020.

Prestación	Objetivo	Condición
i.e. Servidores y sistemas de almacenamiento	Mitigación cambio climático	Los equipos que se utilicen cumplirán los requisitos relacionados con el consumo

	Transición a una economía circular	energético establecidos de acuerdo con la Directiva 2009/125/EC
i.e. Servidores y sistemas de almacenamiento	Transición a una economía circular	Los equipos no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE.

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:

(X) 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.

(X) Por incumplimiento. 5%

(X) Por incumplimiento de las obligaciones asociadas al DNSH del componente/inversión: 2%

() 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:

- a) NIF del contratista y, en su caso de los subcontratistas
- b) Nombre o Razón Social
- c) Domicilio fiscal del contratista y, en su caso, subcontratistas
- d) Aceptación de la cesión de datos entre las Administraciones Públicas implicadas para dar cumplimiento a lo previsto en la normativa europea que es de aplicación y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (Modelo Anexo IV.B de la Orden HFP/1030/2021, de 29 de septiembre)
- e) Declaración responsable relativa al compromiso de cumplimiento de los principios transversales establecidos en el PRTR y que pudieran afectar al ámbito objeto de la gestión (Modelo Anexo IV.C de la Orden HFP/1030/2021, de 29 de septiembre)
- f) Los contratistas acreditarán la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT o en el Censo equivalente de la Administración Tributaria Foral, que debe reflejar la actividad efectivamente desarrollada en la fecha de participación en el procedimiento de licitación.

El propuesto como mejor clasificado, de forma previa a elevar la propuesta de adjudicación, deberá cumplimentar la DECLARACIÓN MULTIPLE en el formato previsto en el apartado B.6 de esta Adenda, relativa a contratos específicos financiados con cargo al Plan de Recuperación, Transformación y Resiliencia (PRTR).