

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 SUMINISTRO DE EQUIPOS DE
COMUNICACIONES, SERVIDORES Y SISTEMAS DE ALMACENAMIENTO -
SDA 24/2022**

(Expediente nº 2022/68)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

**SUMINISTRO E IMPLANTACIÓN DE UNA PLATAFORMA DE
CIBERRESILIENCIA PARA EL SERVICIO MADRILEÑO DE
SALUD**

Lote 2 - Servidores y sistemas de almacenamiento

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 **12 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
3.	DURACIÓN DEL CONTRATO	6
3.1.	Fecha de inicio de la ejecución	6
3.2.	Plazo de entrega de los suministros	6
3.3.	Plazo de ejecución del contrato	7
3.4.	Prórroga del contrato específico	7
4.	VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN	7
4.1.	Presupuesto de licitación y aplicaciones presupuestarias	7
4.2.	Determinación del precio del contrato	9
4.3.	Tramitación del expediente (a efectos presupuestarios)	10
4.4.	Modificación del contrato específico	10
4.5.	Valor estimado	10
4.6.	Contrato financiado con cargo al presupuesto de la Unión Europea	11
4.7.	Entrega de bienes de la misma clase como parte del pago	11
5.	LUGAR Y CONDICIONES DE LA ENTREGA	11
6.	INCOMPATIBILIDADES PARA LA LICITACIÓN	12
7.	CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN	12
7.1.	Ponderación de los criterios de adjudicación	12
7.2.	Fórmula aplicable al criterio precio	13
7.3.	Otros criterios evaluables automáticamente mediante fórmulas, distintos al precio	13
7.3.1.	Criterios relativos al consumo energético de los equipos o su eficiencia energética	13
7.3.2.	Fórmulas para la evaluación automática de los criterios	14
7.4.	Criterios cuya cuantificación depende de un juicio de valor	14
7.4.1.	Criterios y ponderación	14
7.4.2.	Método de valoración y documentación	14
8.	OFERTAS ANORMALMENTE BAJAS	15
9.	CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA	15
9.1.	Obligaciones generales	15
9.2.	Otras condiciones de ejecución del contrato	16
9.3.	Obligaciones de seguridad en cumplimiento del ENS	16
10.	PAGO Y FACTURACIÓN	17
10.1.	Pago del precio	17
10.2.	Condiciones de presentación de las facturas	17
11.	GARANTÍA DE LOS BIENES	18

12.	PENALIDADES	19
12.1.	Penalidades fijadas en el sistema dinámico de adquisición.....	19
12.2.	Fórmula para la aplicación de penalidades.....	19
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	20
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS.....	20
	ANEXO I PRESCRIPCIONES TÉCNICAS.....	22
I.1.	Requisitos funcionales de los suministros	22
I.2.	Requisitos no funcionales de los suministros	34
I.3.	Características de la garantía obligatoria del fabricante.....	34
I.4.	Periodo de vigencia y modalidad de licenciamiento.....	37
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO	39
II.1.	Servicios de instalación avanzada de los suministros	39
II.2.	Servicios de soporte de los suministros.....	43
II.3.	Requisitos de los perfiles profesionales.....	43
	ANEXO III TRATAMIENTOS DE DATOS, FINALIDAD Y MEDIDAS	44
III.1.	Tratamientos de datos y finalidad de los tratamientos	44
III.2.	Medidas técnicas y organizativas	44
	ANEXO IV ENTREGAS PARCIALES	45
	ANEXO V COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO	46
	ANEXO VI MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN	47
	ANEXO VII.....	48
	ANEXO VIII DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA	48
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	51
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea	51
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR	53

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

Organismo destinatario

Unidad proponente: CM – DIRECCIÓN GENERAL DE SALUD DIGITAL

Centro directivo: CONSEJERÍA DE DIGITALIZACIÓN

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

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

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

Datos de **contacto**:

Dirección Postal: C/ Embajadores, 181, 28045 - Madrid

Correo electrónico: dgsd@salud.madrid.org

Teléfono: 913442339

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 2 - Servidores y sistemas de almacenamiento

Título del contrato: SUMINISTRO E IMPLANTACIÓN DE UNA PLATAFORMA DE CIBERRESILIENCIA PARA EL SERVICIO MADRILEÑO DE SALUD.

Objeto del contrato:

El objeto del contrato es el suministro e implantación de una plataforma de Ciberresiliencia que permita tener la capacidad de proteger y defender los datos Sanitarios del Servicio Madrileño de Salud (SERMAS), gestionados por la Dirección General de Salud Digital, ante un ciberataque sobre los entornos en línea de copia de seguridad y repositorios de datos no estructurados. La nueva infraestructura debe garantizar la compatibilidad con las infraestructuras de Backup disponibles.

2.2. CARACTERÍSTICAS PRINCIPALES DE LAS PRESTACIONES

Con respecto a los suministros objeto del contrato específico:

- ☒ Se adquieren equipamientos en infraestructura local
- ☒ Se adquiere software embarcado
- ☐ Se adquiere software con carácter accesorio al suministro de equipamientos

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 V** 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**.

Los suministros llevan asociados de forma obligatoria la **garantía del fabricante** por un periodo de tres años según lo descrito en el apartado III.6 del PPT, sin perjuicio de la garantía adicional que se defina en el **Anexo I.3** y/o la ampliación del periodo máximo de garantía hasta un máximo de 5 años en las condiciones previstas en la invitación.

☒ Se exige el suministro de **soluciones concretas** a fin de garantizar la compatibilidad con las funcionalidades existentes. Se incluye justificación en el expediente.

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

☒ El número de unidades a entregar se define con exactitud en este documento de invitación.

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

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

☒ Las prescripciones técnicas de los suministros se describen en el **Anexo I**.

☒ El contrato requiere servicios de instalación avanzada y/ soporte que se describen en el **Anexo II**.

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

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

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

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

tener acceso en las tareas solicitadas de instalación avanzada descritas para la implantación de la plataforma de CIBERRESILIENCIA solicitada en este documento.

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

☐ El organismo destinatario ha categorizado el sistema o sistemas de información de los que forman parte los bienes suministrados, de la siguiente manera:

- Sistema Haga clic o pulse aquí para escribir texto.: categoría Elija un elemento.
- Sistema Haga clic o pulse aquí para escribir texto.: categoría Elija un elemento.
- Haga clic o pulse aquí para escribir texto.

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

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

Relación de los suministros con la arquitectura de seguridad

☐ Los suministros **no forman parte de la arquitectura de seguridad**

☒ El suministro incluye equipamientos o 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 suministros objeto del presente contrato específico, que forman parte de la arquitectura de seguridad del organismo destinatario son los siguientes²:

Sistemas de protección y copia de seguridad de los datos sanitarios

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 LOS SUMINISTROS

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 suministros es de categoría media o alta.

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

☒ No admite entregas parciales

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

3.3. PLAZO DE EJECUCIÓN DEL CONTRATO

☐ El equipamiento no requiere instalación ni configuración básica. **Plazo máximo** de entrega³: 30 días naturales contados a partir de la fecha de inicio de ejecución del contrato.

☐ Se requiere la instalación y configuración básica de los bienes, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo⁴ de 50 días naturales, incluido el plazo de entrega de los bienes.

☒ 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 los bienes y para la instalación y configuración básica.

- Plazo de ejecución⁵: 8 meses

☐ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario a contar desde el final de la instalación básica, y, en su caso, de la instalación avanzada, descritos en el **Anexo II**, apartado 2, en este caso, el plazo de ejecución total del contrato será de Haga clic o pulse aquí para escribir texto..

En el caso de existir servicios de instalación avanzada y soporte, el **plazo de ejecución** del contrato será el incluido en el cuarto párrafo de este apartado.

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

³ Por defecto, 30 días naturales. El organismo podrá indicar un plazo superior adecuado a las características de los bienes y la situación de abastecimiento de los mercados.

⁴ Por defecto, 50 días naturales. El organismo podrá indicar un plazo superior. Este plazo incluye los 30 días naturales para la entrega de los bienes. 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.

⁵ La duración máxima de los servicios de configuración avanzada y soporte, en ningún caso, podrá exceder del período de garantía del fabricante de los equipos que se suministran.

Presupuesto total sin impuestos (€)	Impuestos indirectos (€)	Presupuesto total con impuestos (€)
2.558.208,11 €	537.223,70 €	3.095.431,81 €

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
SUMINISTRO			
Suministro de equipamientos y, en su caso, software embarcado (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	2.501.368,12 €	525.287,31 €	3.026.655,43 €
Elementos complementarios			
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	56.839,99 €	11.936,40 €	68.776,38 €
Servicio de soporte, a prestar por el adjudicatario			
TOTAL	2.558.208,11 €	537.223,70 €	3.095.431,81 €

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

En todo caso, el importe de los servicios deberá ser inferior al importe de los suministros. Las ofertas que presenten los licitadores no podrán superar el importe presupuestado de los servicios de soporte. Se excluirán las ofertas que no se adecuen a estas estipulaciones.

Las obligaciones económicas que se deriven para la Administración por el cumplimiento del contrato serán financiadas por el Presupuesto de Gastos del organismo Consejería de Digitalización, Centro de Gestión servicios centrales Servicio Madrileño de Salud, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	Anualidad 2024
G/311P/62600 (Hardware)	3.026.655,43 €
G/311P/22703 (Servicios)	68.776,38 €

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	56.839,99 €
Resto costes directos	2.092.914,73 €
Costes indirectos + Gastos generales + Beneficio industrial	408.453,40 €
Total, sin IVA	2.558.208,11 €

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

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

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

Costes de personal							
Perfiles	Dedicación	Salario Base	Especialización tecnológica (48%)	Salario anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 30%
1 CONSULTOR SENIOR (RESPONSABLE DEL SERVICIO) Consultoría desarrollo y sistemas (AREA 3 Grupo A Nivel 1)	10%	28.850,23 €	13.848,11 €	42.698,34 €	4.269,83 €	4.269,83 €	5.550,78 €
1 CONSULTOR SENIOR (Arquitecto sistemas) Consultoría desarrollo y sistemas (AREA 3 Grupo A Nivel 1)	30%	28.850,23 €	13.848,11 €	42.698,34 €	12.809,50 €	12.809,50 €	16.652,35 €
2 técnico de Implantación (AREA 3 Grupo C Nivel 3)	40%	22.503,15 €	10.801,51 €	33.304,66 €	13.321,87 €	26.643,74 €	34.636,85 €

Si bien resulta de aplicación el convenio sectorial, en el presente servicio se requiere una cualificación superior debido a la alta especialización técnica y experiencia requerida en la arquitectura tecnológica y herramientas necesarias para ejecutar los trabajos descritos en este documento con los plazos y calidad exigidos por la DGSD. Dada la naturaleza del entorno y de los datos gestionados, los perfiles Consultor Senior, debe tener cualificación y experiencia en el ámbito de la gestión de la protección de grandes volúmenes de datos y Ciberresiliencia. Así mismo, dadas las características de la arquitectura tecnológica para la gestión de grandes volúmenes de datos, los técnicos de Implantación, deben de disponer de la cualificación y experiencia en entornos de computación y de almacenamiento de entornos de protección de datos. Se estima un porcentaje de especialización técnica del 48 % para los perfiles solicitados, tal y como se refleja en la anterior tabla de costes de personal.

4.3. TRAMITACIÓN DEL EXPEDIENTE (A EFECTOS PRESUPUESTARIOS)

☒ Ordinaria.

☐ Anticipada:

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

4.4. MODIFICACIÓN DEL CONTRATO ESPECÍFICO

☒ **No se prevén modificaciones convencionales** del contrato, todo ello sin perjuicio de los supuestos de modificación legal contemplados en el artículo 205 de la LCSP.

☐ El contrato específico **podrá ser modificado** durante su vigencia, conforme a lo previsto en los artículos 203.a) y 204 LCSP, en un porcentaje máximo del 20% del precio inicial de adjudicación.

Serán de aplicación las siguientes condiciones:

NO APLICA

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 2.558.208,11 euros, según el siguiente desglose:

Valor estimado	Importe (€)
----------------	-------------

Importe total de la prestación, sin IVA	2.558.208,11 €
Importe máximo por modificación prevista, sin IVA	Haga clic o pulse aquí para escribir texto.
TOTAL	2.558.208,11 €

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

- ☒ **SI** está sujeto a regulación armonizada
- ☐ **NO** está sujeto a regulación armonizada

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

- ☐ No.
- ☒ Sí. Instrumento /Fondo/Programa/Mecanismo: NEXT GENERATION EU - MECANISMO DE RECUPERACIÓN Y RESILIENCIA. PLAN DE RECUPERACIÓN, TRANSFORMACION Y RESILIENCIA/POLÍTICA PALANCA IV/COMPONENTE 11/INVERSIÓN 3.

Código de operación/Proyecto/Iniciativa: "GRUPO 1.1.2 COPIA OFFLINE"

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.

4.7. ENTREGA DE BIENES DE LA MISMA CLASE COMO PARTE DEL PAGO

- ☐ Sí.
- ☒ No.

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) - CPD ATHENE@ en Hospital Universitario 12 de octubre. DIRECCIÓN GENERAL DE SALUD DIGITAL - Consejería de Digitalización - Comunidad de Madrid - C/ Doctor Tolosa Latour S/N - Sala Athenea – Planta 1 28041 Madrid.
- Correo electrónico: direccion.cedas@salud.madrid.org
- Teléfono: 626661756 / 615043824
- Fax: Haga clic o pulse aquí para escribir texto.

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

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

☒ Solo se utilizan el precio, el criterio de consumo energético y otros criterios evaluables mediante fórmulas, con los siguientes pesos:

Criterio de ahorro o eficiencia energética	Precio	Otros criterios evaluables mediante fórmula
5%.	95%	NO APLICA

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

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

SOBRE 1. Criterios que dependen de un juicio de valor	SOBRE 2.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 2.2. Precio
Haga clic o pulse aquí para escribir texto.	5 puntos	95 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 y también si se quiere dar preponderancia en la adjudicación al precio del contrato, aunque todos los criterios sean evaluables mediante fórmula):

$$C_i = P * \frac{O_l - O_i}{O_l - O_b}$$

Donde:

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

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

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

O_b , es el precio más bajo ofertado (IVA excluido)

O_l , es el presupuesto máximo de licitación (IVA excluido)

☒ Función **minimizar precio** (se puede utilizar si sólo se utilizan criterios automáticos y se quieren valorar todos los criterios objetivos de forma proporcional):

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

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 RELATIVOS AL CONSUMO ENERGÉTICO DE LOS EQUIPOS O SU EFICIENCIA ENERGÉTICA

La plataforma presentada debe ser eficiente energéticamente, y cumplir con las normativas de consumo responsable, para ello se solicita que el licitador presente el certificado Energy Star para cada uno de los equipos presentados en su propuesta.

CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓN
Plataforma Certificada Energy Star: Toda la plataforma presentada debe de disponer del Certificado Energy Star.	5	Sí/No

7.3.2. FÓRMULAS PARA LA EVALUACIÓN AUTOMÁTICA DE LOS CRITERIOS

Función Maximizar:

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

Donde:

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

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

Función Minimizar:

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

Donde:

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

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

Función Sí/No (maximizar binario):

$$X_i = P$$

Donde:

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

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

7.4.1. CRITERIOS Y PONDERACIÓN

NO APLICA

7.4.2. MÉTODO DE VALORACIÓN Y DOCUMENTACIÓN

NO APLICA

8. OFERTAS ANORMALMENTE BAJAS

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

- Si existiendo 4 o más licitadores las ofertas económicas presentadas resultan inferiores en más de 20 unidades porcentuales a la media aritmética de las ofertas presentadas. No obstante, si entre ellas existen ofertas que sean superiores a dicha media en más de 20 unidades porcentuales, se procederá al cálculo de una nueva media sólo con las ofertas que no se encuentren en el supuesto indicado. En todo caso, si el número de las restantes ofertas es inferior a tres, la nueva media se calculará sobre las tres ofertas de menor cuantía. Si, por el contrario, han concurrido menos de cuatro licitadores, resultarán de aplicación las previsiones del artículo 85 apartados 1 a 3 del Reglamento 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas.
- A la condición anterior, siempre que existan criterios diferentes al precio, se deberá añadir la siguiente para apreciar el carácter anormal o desproporcionado de las ofertas.
 - ☐ Cuando la puntuación en el criterio de calidad de mayor peso de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media de los valores ofertados:
 - ☒ 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 productos con distribución comercial, no pudiendo aplicar precios superiores a los de mercado conforme a las condiciones del apartado 17.2 b) 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 distribuir únicamente equipamientos que cumplan lo previsto en el apartado III.3 del PPT.
- 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 equipos o 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 incluidos en el equipo ofertado, en cumplimiento de la medida [op.pl.5.r2.1] del ENS.

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

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

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

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

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

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

10.2. CONDICIONES DE PRESENTACIÓN DE LAS FACTURAS

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

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

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

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

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

- Campo <FileReference>: SDA 24/2022.

- 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
- Órgano responsable del contrato específico: Dirección General de Salud Digital - A13002908
- Órgano gestor: 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 26/2021.
- 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 los suministros, 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 **garantía obligatoria del fabricante** del apartado III.6 del PPT, que será de 3 años o un plazo superior (hasta 5 años) según lo previsto en el documento de invitación (Anexo I.3) o el ofrecido por el adjudicatario, en su caso.

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 V** de este documento, cuya duración se extenderá durante todo el periodo de garantía obligatoria del fabricante de los bienes.

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 PLACSP⁷ u otra plataforma de contratación a disposición del organismo.

Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa⁸.

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

La oferta económica deberá incluir, al menos, la información en el modelo de oferta disponible en el Portal de Contratación Centralizada para el SDA 24/2022, en la siguiente dirección: <https://contratacioncentralizada.gob.es/documents/11614/218482/Modelos+de+Oferta+SDA+24+2022.zip/f0d2567b-725b-4221-bec1-ac5c0287edb4>. 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 equipos y/o programas que se ofertan
- La información de los requisitos mínimos de los productos o referencias a las fichas técnicas o catálogos que permitan acreditar los criterios automáticos:
 - Cumplimiento de Requisitos Anexo I y Anexo II
- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - **NO APLICA**
- Si la oferta incluye equipos y/o 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

⁷ Las ofertas se presentarán a través de LICIT@, disponible en el Portal de la Contratación de la Comunidad de Madrid. El enlace de acceso es:

https://gestion5.madrid.org:8203/sap/bc/webdynpro/sap/zfrms_wd_le_003#

⁸ 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.

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, PREVALECEERÁN ESTOS ÚLTIMOS.

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

EL TITULAR DEL ÓRGANO DESTINATARIO (CARGO): LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado electrónicamente (nombre y apellidos): Nuria Ruiz Hombrebueno

Firmado digitalmente por: RUIZ HOMBREBUENO NURIA
Fecha: 2024.05.31 09:29

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS SUMINISTROS

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) (CPD Athene@, en Hospital Universitario 12 de Octubre, CPD de la calle Aduana 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 de 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.

Hoy la pérdida de funcionalidad de dichos servicios TIC puede suponer poner en peligro la continuidad asistencial pública sanitaria a los ciudadanos, e incluso podría afectar a la salud de los pacientes.

Por tanto, los sistemas de información ubicados en los Centros de Proceso de Datos centrales de la DGSD, que utilizan los profesionales del ámbito sanitario y los ciudadanos de la Comunidad de Madrid, necesitan una protección adicional de los datos críticos frente a las copias de seguridad realizadas de modo “tradicional” a través de la infraestructura “en línea” ante un ataque cibernético.

El objeto del presente contrato es el suministro de una plataforma de Ciberresiliencia que permita tener la capacidad de proteger y defender los datos sanitarios ante un ciberataque, aislando física y lógicamente los datos, protegiéndolos de los ataques y automatizando las fases básicas del proceso de recuperación.

Sin esta infraestructura protección ante un desastre natural, ciberataque o malfuncionamiento no esperado, se podría perder información crítica para la actividad asistencial y adicionalmente, se incumpliría la normativa legal vigente en materia de Protección de Datos de Carácter Personal y Esquema Nacional de Seguridad, al no disponer de copias de seguridad fuera de línea que permitieran recuperar la información ante un desastre.

Actualmente la DGSD dispone de cuatro dispositivos IDPA (Integrated Data Protection Appliance) del fabricante Dell Technologies, en concreto, dos dispositivos IDPA 5800 y dos dispositivos IDPA 8300, replicadas, que alojan las copias de seguridad o backup de los datos

gestionados por los profesionales sanitarios en el uso normal de las aplicaciones y sistemas de información alojados en los CPD corporativos.

Así mismo se dispone de dos clústeres de sistemas de almacenamiento de archivos conectado en red (NAS) de escalamiento horizontal replicados, formados por 15 nodos en cada uno de los clústeres de la familia POWERSCALE anteriormente ISILON del fabricante Dell Technologies. Los cuales alojan los datos no estructurados de las imágenes radiológicas y no radiológicas y otros tipos de datos críticos en sistemas de ficheros.

Los cuales tienen las siguientes características.

- **2 dispositivos IDPA 5800 cada uno con.**
 - 240 TB físicos Brutos y 183 TB físicos Netos.

Los cuales alojan las copias de seguridad de un volumen de datos de 19,6 PB lógicos con una ratio de deduplicación de 116:1

- **2 dispositivos IDPA 8300 cada uno con.**
 - 300 TB físicos Brutos y 228 TB físicos Netos.

Los cuales alojan las copias de seguridad de un volumen de datos de 11,4 PB lógicos con una ratio de deduplicación de 37:1.

- **Clústeres de datos no Estructurados**

Cada uno de los en los dos clústeres del sistema de almacenamiento NAS de escalamiento horizontal del proporcionan una capacidad neta de 750 TiB netos usables sin contar con las funcionalidades adicionales de compresión y deduplicación en cada uno de los dos sistemas.

A nivel de software de copia de seguridad la DGSD dispone del sistema integrado Data Protection Suite en los dispositivos IDPA con la capacidad de licenciamiento asociada al volumen físico de cada uno de los dispositivos.

Por tanto, se solicita una solución completa de Ciberresiliencia a implantar en el CPD Central de la DGSD, la cual será capaz de proteger los datos contra un ataque cibernético, aislando los datos de copia de seguridad, protegiéndolos contra dichos ataques, y automatizando las fases básicas del proceso de recuperación.

En resumen, esta solución de Ciberresiliencia cumplirá con los siguientes requisitos funcionales:

- Deberá ser completamente compatible con los entornos de backup actuales para el dato estructurado y con los sistemas de almacenamiento para el dato no estructurado.
- Almacenar de forma segura todos los backups productivos en un entorno aislado, en adelante “Vault”.
- Ofrecer herramientas de análisis, verificación y ayuda en el punto de recuperación limpio de ataques ransomware.

- Automatizar la restauración de servidores de backup para que ésta sea más sencilla y rápida, reduciendo así el tiempo de recuperación (RTO).
- Ser capaz de conectar el entorno seguro Vault con la red de producción en caso necesario para una eventual recuperación de datos.
- Requiera de credenciales de seguridad independientes y autenticación multifactor para acceder.

La integración de esta nueva plataforma se realizará tanto a nivel de software como a nivel de hardware teniendo en cuenta los repositorios informáticos de los que dispone la DGSD.

A continuación, se describirá como se realizará esa integración a grandes rasgos:

La solución deberá ser capaz de recuperar los sistemas productivos de copia de seguridad y de datos no estructurados, así como la evolución de estos sistemas en origen.

A nivel de hardware, el sistema deberá integrarse de forma nativa con los actuales equipos IDPA que dan servicio a la DGSD, así como con los sistemas de datos no estructurados y permitirá la creación de repositorios unificados con toda la información a proteger en los distintos Vault. De esta forma se posibilitará la continuidad de la protección de los datos, con el actual nivel de servicio y teniendo en cuenta el continuo crecimiento de todos los servicios y aplicativos prestados.

Diariamente se realizará una copia incremental de un entorno a otro por conexión directa de Fibra Óptica y se almacenarán los cambios en los nuevos dispositivos que se integrarán de forma nativa con los dispositivos actuales.

A esta copia incremental se le aplicará una configuración de forma que esos backups o los datos no estructurados sean inmutables, es decir, no será posible su modificación o borrado alguno, ni siquiera por parte de los administradores de la plataforma, durante un periodo estipulado de tiempo. De forma paralela, se accederá a un entorno controlado o sandbox en el que se analizarán esos cambios diarios para poder establecer patrones de comportamiento habituales y poder distinguirlos de casuísticas extrañas que potencialmente sean indicativas de estar sufriendo un ciberataque.

Es clave que los Vault sea capaces de realizar copias nativas deduplicadas, debido a la muy alta volumetría de datos lógicos protegidos en los sistemas productivos, así como que la capacidad del software de análisis, de entender los datos almacenados por el software de backup y de los entornos de ficheros y restaurar datos desde los vault hacia los entornos de producción asociados en caso de desastre.

La nueva plataforma permitirá la automatización del proceso de copia al Vault, iniciado siempre desde el Vault, sin conocimiento de una copia aislada por parte de las aplicaciones o del software de Backup productivo.

Se diferenciarán los siguientes tipos de componentes de suministro para formar la plataforma de Ciberresiliencia de la DGSD:

1. Plataforma de Ciberresiliencia para el Dato Estructurado en sistemas de Copia de Seguridad.

1.1. Ampliación de la capacidad de almacenamiento en los appliances de almacenamiento de backup a disco deduplicado para la copia de seguridad y restauración.

Como ya se explica en este documento la DGSD dispone de cuatro dispositivos que alojan las copias de seguridad o backup de los ficheros y protección de archivo de los datos gestionados por los profesionales sanitarios en el uso normal de las aplicaciones y sistemas de información alojados en los CPD corporativos.

Estos sistemas necesitan ampliación de capacidad de almacenamiento para poder asumir el crecimiento vegetativo de los datos generados en los sistemas en producción el crecimiento derivado de la puesta en producción de nuevos servicios y sistemas de información sanitarios centralizados, marcados en objetivos y actuaciones globales planteados dentro del plan de Salud Digital realizado por la DGSD.

En concreto, se solicitan las siguientes ampliaciones:

- **Ampliación de disco para los dos sistemas IDPA 5800 o equivalente. 60 TiB Brutos para cada una de las cabinas.**
 - CPD ADUANA: 15 discos de 4TB sobre bandeja existente.
 - CPD ATHENE@: 15 discos de 4TB sobre bandeja existente.

Lo que ofrece una capacidad de 60 TB brutos para cada una de las dos appliances.

- **Ampliación de disco para los dos sistemas IDPA 8300 o equivalente. 60 TiB Brutos para cada una de las cabinas.**
 - CPD ADUANA: 15 discos de 4TB sobre bandeja existente.
 - CPD ATHENE@: 15 discos de 4TB sobre bandeja existente.

Lo que ofrece una capacidad adicional de 60 TB brutos para cada una de las dos appliances

La ampliación conlleva las ampliaciones correspondientes del licenciamiento para cada uno de los sistemas, por tanto, debe suministrarse con todas las funcionalidades de software activadas para toda la nueva capacidad solicitada.

Las funcionalidades son las siguientes:

- Ampliación del Software de los Sistemas con las funcionalidades que activan la inteligencia de dichos dispositivos entre ellas:
 - Funcionalidad que habilita que la plataforma ofrezca almacenamiento con protección habilitado para la nube, escalable y de alta velocidad para respaldo, archivo y recuperación ante desastres.
 - Funcionalidad para deduplicar datos en línea durante los procesos de respaldo o archivado, lo que maximiza el rendimiento de respaldo y, al mismo tiempo, minimiza los requisitos de almacenamiento en disco.

- Verificación de datos de punto a punto: Las verificaciones de punto a punto implican la lectura de los datos después de su escritura y su comparación con los datos enviados al disco, siempre que se pueda acceder a ellos por medio del sistema de archivos en disco y que los datos no estén dañados.
 - Protección mediante el cifrado que se ejecuta en línea (antes de escribir los datos en el disco).
 - Admitir simultáneamente varios métodos de acceso, incluidos NFS, CIFS, VTL, NDMP.
 - Implementar políticas de gobierno corporativo internas o normativas de cumplimiento de normas para datos de archivo. Permite a los administradores de almacenamiento, a los administradores de respaldo y a los directores de cumplimiento de normas satisfacer los requisitos de retención de datos para los datos almacenados en estos sistemas. Impide que los archivos se modifiquen o se eliminen durante un período de retención definido por el usuario.
 - Funcionalidad de replicación de datos a un sitio de recuperación ante desastres en datos comprimidos únicos mediante la red, lo que requiere una fracción del tiempo, el ancho de banda y el costo que implican los métodos de replicación tradicionales.
 - Organizar los datos en niveles de manera nativa en la nube pública, privada o híbrida para retención a largo plazo. Los datos que se depositan en el almacenamiento de objetos de nube que ya está deduplicado.
 - Función automática de creación de informes del sistema Call Home, denominada soporte automático, que proporciona notificación por correo electrónico del estado del sistema completo al servicio de soporte.
- Ampliación del Software de Protección de Datos, integrado en dichos sistemas los cuales activan las siguientes funcionalidades:
- Data Manager: Gobierno corporativo de TI, autoservicio, agilidad operativa, deduplicación y protección de datos definida por software para entornos de nube, físicos y virtuales:
 - Proporciona administración de datos flexible y cumplimiento entre aplicaciones y entornos de TI nativos en la nube.
 - Respallos y restauraciones directamente desde las aplicaciones nativas.
 - Optimizado para nube múltiple.
 - Administración basada en SaaS.
 - Respaldo y recuperación rápidos y eficientes mediante tecnología de deduplicación de longitud variable integrada. Optimizado para realizar respaldos completos diarios y rápidos de entornos físicos y virtuales, servidores

NAS, aplicaciones empresariales, oficinas remotas y equipos de escritorio/laptops.

- Respaldo y recuperación unificados para la empresa: deduplicación, respaldo en disco y en cinta, instantáneas, replicación y NAS. Protege los entornos físicos y virtuales, incluidos VMware y Microsoft Hyper-V.
- Recuperación rápida de máquinas virtuales de VMware a cualquier punto en el tiempo, proporciona protección continua de datos (CDP) para la recuperación operacional y la recuperación ante desastres.
 - Protección de máquinas virtuales de VMware con recuperación granular al nivel de una máquina virtual.
 - Replica de máquinas virtuales (VMDK y RDM) de manera local y remota
 - Es compatible con cualquier arreglo de almacenamiento en la lista de compatibilidad de hardware (HCL) de VMware.
 - Optimiza el uso del ancho de banda WAN con compresión de datos y deduplicación.

1.2. Dos equipos integrados de backup deduplicado (PBBA - Purpose Built Backup Appliance) o equivalente.

Se suministrarán dos equipos integrados (PBBA) en total que permitan consolidar los datos para Vault de forma aislada para cada uno de los distintos dispositivos IDPA actuales de la DGSD (IDPA8300 y IDPA 5800) y sus ampliaciones solicitadas en este documento. En Adelante Vault Servicios Centrales y Vault Athene@.

1.2.1. Vault del entorno Servicios Centrales:

Se tratará de un dispositivo PBBA de características especialmente diseñadas para un uso eficiente en la copia de seguridad, con deduplicación, compresión y protección.

Este equipo tendrá al menos 960 TB Brutos físicos (antes de la deduplicación, compresión y protección), a partir de discos de al menos 8TB. Dispondrá adicionalmente de discos de tecnología SSD para mejorar el rendimiento de las recuperaciones de entornos virtuales.

Debe permitir la replicación nativa y directa, de forma deduplicada entre los sistemas actuales de producción y el nuevo PBBA ofertado.

1.2.2. Vault del entorno Athene@:

Se tratará de un dispositivo PBBA de características especialmente diseñadas para un uso eficiente en la copia de seguridad, con deduplicación, compresión y protección.

Este equipo tendrá al menos 720 TB Brutos físicos (antes de la deduplicación, compresión y protección), a partir de discos de al menos 8TB. Dispondrá adicionalmente de discos de tecnología SSD para mejorar el rendimiento de las recuperaciones de entornos virtuales.

Debe permitir la replicación nativa y directa, de forma deduplicada entre los sistemas actuales de producción y el nuevo PBBA ofertado.

Los dispositivos contarán con licenciamiento para todas las funcionalidades, exceptuando la funcionalidad para el desborde a nube para toda la capacidad ofertada.

1.3. Software de automatización de copia de datos al Vault.

Es el responsable de realizar las réplicas de los entornos de una forma segura y automatizada. Deberá ser capaz de realizar esta réplica desde múltiples repositorios de datos desde los dispositivos de origen de la DGSD hacia los nuevos dispositivos de Vault.

Será capaz de lanzar la recuperación automática desde los servidores backup que prestan servicio a la plataforma actual, así como de programar trabajos diarios que analicen los datos obtenidos.

Este software estará virtualizado dentro del Vault y se instalará en una versión compatible con los softwares de los entornos de producción.

Se suministrarán todas las licencias necesarias para su funcionamiento con la infraestructura actual de la DGSD anteriormente descrita.

1.4. Software de análisis de comportamientos inusuales.

Este software es responsable de la monitorización de los datos corporativos (a partir de las réplicas periódicas del backup residentes en el Vault), el análisis de estos y con la ayuda del uso de inteligencia artificial, será capaz de aprender los patrones de comportamiento estándar de la organización para distinguirlos de los anómalos. Alertará sobre dichos comportamientos inusuales que sean indicativos de un ciberataque: archivos corruptos o cifrados, creación o borrado masivo e inusual de archivos y diferencias de entropía en ficheros, entre otros.

A diferencia de un software antivirus tradicional, basado en la continua actualización de su base de datos de patrones de amenazas, este software se encuentra aislado dentro del Vault, y no requiere de dichas actualizaciones. Esto no implica que este software sea invariable, pues deberá contar con las debidas actualizaciones de versiones que corrijan errores y amplíen nuevos métodos de detección de patrones. En cualquier caso, la actualización de versión de este software, al igual que el resto de los elementos software dentro del Vault, deberán realizarse de una manera manual y procedimentada al no disponer de conexión a Internet.

Este software se integrará con el software de automatización de copia de datos al Vault para poder llevar a cabo su chequeo automático después de cada copia de seguridad realizada en el entorno de Vault.

Se dispondrá de licencia para analizar al menos 275 TBs de información en frontal del entorno de producción del actual de la DGSD IDPA 8300 y de licencia para analizar al menos 175 TBs de información en frontal del entorno de producción actual IDPA5800.

1.5. Switches de comunicaciones.

Cada una de las dos plataformas de Vault incorporaran dos switches de comunicaciones certificados para la solución, para poder interconectar los elementos ofertados.

1.6. Servidores de análisis y control del entorno de Vault.

1.6.1. Entorno de Vault Servicios Centrales:

Se trata de servidores con capacidad de cómputo suficiente para el análisis de la seguridad, detección temprana, recuperación rápida de un ataque cibernético y gestionar el entorno de Vault Servicios Centrales.

- 5 servidores enracables de 1U certificados para la solución ofertada para el análisis de los datos cada uno con:
 - 2 procesadores Intel Xeon Gold 5218 o equivalente (16 cores, 2,3 GHz) o superior.
 - 384 GB RAM (en módulos de 32 GB RDIMM).
 - 2 discos SSD M.2 480 GB RAID 1 Arranque Sistema Operativo
 - 10 discos SAS de 2,4 TB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 2 puertos 10/25 GB SFP28
 - 1 tarjeta de 4 puertos 10GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencias de Gestión avanzada.
 - Licencias embebidas VMware vSphere 8 Standard o equivalente/superior
- 1 servidor enracable de 1U certificado para la solución ofertada, para ejecutar el software de automatización del Vault con:
 - 2 procesadores Intel Xeon Gold 5218 o equivalente (16 cores, 2,3 GHz) o superior.
 - 192 GB RAM (en módulos de 16 GB RDIMM).
 - 2 discos SSD M.2 480 GB RAID 1 Arranque Sistema Operativo
 - 10 discos SAS de 2,4 TB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 2 puertos 10/25 GB SFP28
 - 1 tarjeta de 4 puertos 10GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencias de Gestión avanzada.
 - Licencias embebidas VMware vSphere 8 Standard o equivalente o superior
- 1 servidor certificado para la solución ofertada, para ejecutar el entorno de administración del Vault con:
 - 1 procesador Intel Xeon E- 2334 o equivalente (4 cores, 3,4 GHz) o superior.
 - 16 GB RAM (en módulos de 16 GB RDIMM).
 - 2 discos SSD de 960 GB

- 1 tarjeta Controladora RAID 12G
- 1 tarjeta de 2 puertos 10/25 GB SFP28
- 1 tarjeta de 4 puertos 10GE Base -T
- 2 puertos 1GB Base -T
- Doble fuente de alimentación
- Licencias de Gestión avanzada.

Se requiere el despliegue del software de automatización de copia de datos al Vault y el de análisis de comportamientos inusuales en esta infraestructura.

1.6.2. Entorno de Vault Athenea:

Se trata de servidores con capacidad de cómputo suficiente para el análisis de la seguridad, detección temprana, recuperación rápida de un ataque cibernético y gestionar el entorno de Vault Athene@.

- 4 servidores enracables de 1U certificados para la solución ofertada para el análisis de los datos cada uno con:
 - 2 procesadores Intel Xeon Gold 5218 o equivalente (16 cores, 2,3 GHz) o superior.
 - 384 GB RAM (en módulos de 32 GB RDIMM).
 - 2 discos SSD M.2 480 GB RAID 1 Arranque Sistema Operativo
 - 10 discos SAS de 2,4 TB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 2 puertos 10/25 GB SFP28
 - 1 tarjeta de 4 puertos 10GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencias de Gestión avanzada.
 - Licencias embebidas VMware vSphere 8 Standard o equivalente/superior
- 1 servidor enracable de 1U certificado para la solución ofertada, para ejecutar el software de automatización del Vault con:
 - 2 procesadores Intel Xeon Gold 5218 o equivalente (16 cores, 2,3 GHz) o superior.
 - 192 GB RAM (en módulos de 16 GB RDIMM).
 - 2 discos SSD M.2 480 GB RAID 1 Arranque Sistema Operativo
 - 10 discos SAS de 2,4 TB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 2 puertos 10/25 GB SFP28
 - 1 tarjeta de 4 puertos 10GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencias de Gestión avanzada.

- Licencias embebidas VMware vSphere 8 Standard o equivalente o superior
- 1 servidor certificado para la solución ofertada, para ejecutar el entorno de administración del Vault con:
 - 1 procesador Intel Xeon E- 2334 o equivalente (4 cores, 3,4 GHz) o superior.
 - 16 GB RAM (en módulos de 16 GB RDIMM).
 - 2 discos SSD de 960 GB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 2 puertos 10/25 GB SFP28
 - 1 tarjeta de 4 puertos 10GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencias de Gestión avanzada.

Se requiere el despliegue del software de automatización de copia de datos al Vault y el de análisis de comportamientos inusuales en esta infraestructura.

2. Plataforma de Ciberresiliencia para el dato no estructurado.

La arquitectura propuesta debe contemplar y cumplir con los siguientes apartados generales:

2.1. Sistema de almacenamiento NAS /objeto de escalamiento horizontal para el vault del dato no estructurado

Se trata del suministro de un nuevo sistema NAS de escalamiento horizontal, independiente de los sistemas de ficheros Isilon/PowerScale actuales, para dotar a la solución de capacidad de crear el vault para datos no estructurados. Este sistema será capaz de mantener la producción mínima esencial en caso de fallo de los sistemas productivos indicados en este documento, o bien mantendrá una copia limpia y consistente de la información mínima viable para realizar una restauración.

El nuevo sistema estará formado por al menos un clúster formado por 4 nodos que proporcione una capacidad neta ampliada estimada de 490 TiB netos usables sin contar con las funcionalidades adicionales de compresión y deduplicación. El detalle de suministro para cada uno de los nodos que formaran el clúster es el siguiente:

- CLUSTER VAULT DATO NO ESTRUCTURADO: 4 nodos cada uno con la siguiente configuración:
 - 96 GB de Cache RAM no Volátil (NVRAM).
 - 1 disco SAS SSD 800 GB.
 - 15 discos HDD de 12 TB.

- 2 puertos 25GbitE SFP28 para conectividad backend (compatibles con 10/25GbitE). redundantes
- 2 puertos 25GbitE SFP28 para conectividad frontend (compatibles con 10/25GbitE). redundantes
- Doble fuente de Alimentación.
- Transceiver correspondientes para interconexión con los clústeres de la DGSD.
- Licencia de Gestión avanzada.
- Cableado Eléctrico y de Datos necesarios para la interconexión.

Así mismo se suministrará la electrónica de red para la interconexión Back-end de hasta 100 GBE de los nodos en configuración de alta disponibilidad, actualizables y sustituibles en caliente junto con todo el cableado necesario.

La ampliación conlleva las ampliaciones correspondientes del licenciamiento Software que de soporte a la nueva capacidad con las siguientes funcionalidades solicitadas:

- **Gestión:** Licencia SW básico que incluye las funcionalidades S3, CIFS, NFS, FTP, NDMP, Balanceo de Carga, Aceleración del rendimiento, y protección de Antivirus.
- **Replica de datos nativa y Cifrada:** Modulo con licencia que Habilita la capacidad Replica de cifrada de forma segura de conjuntos de datos en múltiples sitios para una recuperación confiable ante desastres, conmutación por error y conmutación por recuperación.
- **Snap:** Modulo con licencia que habilita la capacidad de protección de los datos de manera eficiente y acelerar la recuperación de datos críticos con restauraciones de instantáneas bajo demanda.
- **Deduplicación:** Modulo con licencia que permite aumentar la eficiencia y reducir los requisitos de capacidad de almacenamiento con deduplicación de datos redundantes en múltiples fuentes.
- **Equilibrio de carga:** Modulo con licencia que Habilita la capacidad de equilibrio de carga, la conmutación por error dinámica y la conmutación por recuperación de las conexiones del cliente.

2.2. Entorno de análisis y protección de seguridad y control del entorno de Vault para datos no estructurados.

Se trata del entorno para el análisis de la seguridad, detección temprana, recuperación rápida de un ataque cibernético y gestión y control del entorno de Vault para datos no estructurados.

Para ello, es necesario que la solución incluya los siguientes elementos:

- 1 servidor enracable de 1U certificados para la solución ofertada para el análisis de los datos cada uno con:
 - 1 procesador Intel Xeon Silver 4309Y o equivalente (8 cores, 2,8 GHz) o superior.
 - 32 GB RAM
 - 2 discos SSD de 3,84 TB
 - 1 tarjeta Controladora RAID 12G
 - 1 tarjeta de 4 puertos 1GE Base -T
 - 2 puertos 1GB Base -T
 - Doble fuente de alimentación
 - Licencia de Gestión avanzada.
 - Licencia VMware vSphere 8 Standard o equivalente/superior

Así mismo, se requiere que la solución incorpore software para el análisis de seguridad y control del entorno vault de datos no estructurados que cumpla con los siguientes requisitos y funcionalidades:

Software de Análisis y protección de seguridad.

Se requiere que el software para el análisis y protección de seguridad ante ataques tipo “ransomware” y similares cumpla con los siguientes requisitos y funcionalidades:

- Debe poder instalarse de forma “virtual appliance” en el entorno actual de virtualización de la DGSD.
- Debe estar licenciado para la totalidad del almacenamiento tanto de los sistemas de producción del dato no estructurado de la DGSD, como también para el nuevo sistema de vault propuesto.
- Incluirá modo de funcionamiento totalmente automatizado basado en aprendizaje: personalizar los ajustes basándose en la supervisión de los patrones de entrada/salida de datos del usuario.
- Deberá integrarse con los sistemas de vault propuestos.
- La solución propuesta no deberá implementarse en modo “proxy” o “man-in-the-middle”, es decir, no deberá instalarse como un agente intermedio interceptando las comunicaciones entre los usuarios/aplicaciones y los sistemas de almacenamiento, sino que deberá implementar los métodos necesarios para proteger el sistema sin emplear ese tipo de mecanismos intrusivos.
- Deberá contar con algún modo de ataque simulado de “ransomware” con el fin de validar que las acciones de respuesta a un ataque funcionan según lo esperado, con alertas enviadas a los administradores para garantizar que todos los componentes de seguridad están listos y se prueban a diario.
- En caso de detectar un ataque, debe ser capaz de registrar e informar de la ruta del usuario, archivo y recursos compartido, dirección IP donde se originó el ataque, y capturar al menos la última hora de actividad del usuario antes del ataque.
- Debe contar con la posibilidad de configurar reglas personalizables para ajustar los falsos positivos, así como la configuración de “listas blancas” para la exclusión de ciertos usuarios y/o aplicaciones de los análisis en tiempo real.

Software de control del Entorno Vault de datos no estructurados

Se requiere que el software de Control del Sistema cumpla con los siguientes requisitos y funcionalidades:

- Debe poder instalarse en formato “virtual appliance” sobre el hardware suministrado descrito anteriormente.
- Licenciado para la totalidad del almacenamiento útil disponible en el sistema de vault para datos no estructurados objeto de suministro.
- Debe poder gestionar autónomamente la comunicación entre el sistema de vault de datos no estructurado y los sistemas productivos asociados indicados en este documento de tal forma que la comunicación de datos se inicie desde el sistema de vault y cuando éste verifique que no existen amenazas o ataques en curso, debe poder cortar la comunicación con los sistemas productivos en cuanto se detecte una amenaza en curso.
- Debe poder enviar un informe de forma automática (periódica) con detalle de los datos copiados hacia el sistema de vault de datos no estructurados y monitorizar la copia de datos.
- En caso de que los sistemas productivos sufran un ataque tipo “ransomware”, “locker”, o similar, el sistema de vault debe poder permitir los siguientes modos de funcionamiento:
 - Mantener una copia consistente e inmutable de los datos con la opción de copiar los datos de vuelta a los sistemas productivos, manteniendo intacta la copia del vault.
 - Permitir prestar el servicio de datos directamente desde el sistema de vault posibilitando así la inmediata prestación del servicio, aunque de esta forma no se pueda mantener intacta la copia del vault.

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

No serán admisibles en ningún caso soluciones de puesta a disposición de activos en la nube. Sólo estará permitida la conexión técnica a la nube de los equipos en los términos descritos en el apartado III.5 del PPT. Los licitadores se comprometen a que los equipos ofertados cumplen con las condiciones y límites definidos para este tipo de conexiones.

I.2. REQUISITOS NO FUNCIONALES DE LOS SUMINISTROS

Los equipamientos suministrados deberán ser conformes con las previsiones recogidas en el apartado III.3 del PPT en materia de marcado CE y acreditación de los requisitos aplicables para su comercialización en la Unión Europea, así como el cumplimiento de la normativa española y europea que sea de aplicación a los mismos en relación a la comercialización de material eléctrico, compatibilidad electromagnética, seguridad de los productos, diseño ecológico, etc.

I.3. CARACTERÍSTICAS DE LA GARANTÍA OBLIGATORIA DEL FABRICANTE

Todos los equipos suministrados están sujetos a una garantía que debe proporcionar el fabricante y que contará, como mínimo, con las siguientes características básicas, según queda recogido en el PPT:

- La garantía obligatoria del fabricante responderá del malfuncionamiento y averías de los equipos.
- El fabricante ofrecerá la posibilidad de recibir avisos en horario de 9h a 17h de lunes a viernes, salvo festivos nacionales. El tiempo máximo de respuesta del fabricante será de 8h dentro de este horario, y el tiempo máximo de reparación de la avería desde la comunicación de la incidencia por el organismo será de 5 días laborables según el calendario laboral aplicable en el lugar donde están instalados los equipamientos.
- Periodo de garantía mínimo de 3 años.

Adicionalmente, se solicitan la siguiente ampliación de las características de la garantía básica:

- ☒ Ampliación de horarios de soporte: 24 horas x 7 días a la semana 365 días al año con tiempo de resolución de 4 horas.
- ☒ Reducción de los tiempos de respuesta: se incluye tabla de tiempos de respuesta
- ☒ Reducción de los tiempos de resolución: Tiempo de resolución de 4 horas para incidencias de nivel 1
- ☒ Periodo de garantía superior: 4 años
- ☒ Otras condiciones adicionales exigibles al fabricante:

La fecha de inicio del servicio de garantía comenzará a partir de la fecha de aceptación del equipamiento, que coincidirá con la instalación y aceptación de los activos (hardware y/funcionalidades software adheridas) en su ubicación final por el centro destinatario.

- La actuación para las incidencias de la infraestructura hardware se llevará a cabo in situ, es decir, en el lugar en el que esté instalado el elemento.
- El adjudicatario será responsable de los elementos objeto de la garantía in situ, y en caso de que se produzca cualquier incidencia en relación con los mismos deberá articular los mecanismos que sean necesarios para su resolución.

Dependiendo de la complejidad, se evaluará la viabilidad de solventarlo con la sustitución del elemento averiado por otro de iguales o superiores características, original del fabricante y compatible con la infraestructura instalada, hasta que se haya producido la reparación del elemento averiado. En este caso, el adjudicatario deberá asegurar que se presta el servicio con total normalidad tras la sustitución.

El fabricante dispondrá de un stock mínimo de materiales/piezas/equipos que le permita garantizar el cumplimiento de los tiempos máximos de resolución de incidencias.

- En cuanto al software, y siempre que se refiera a recursos dentro del ámbito del proyecto, el fabricante deberá proporcionar el derecho de actualización a nuevas versiones del producto y la disponibilidad de parches y revisiones menores, siempre y cuando sea necesario, en cualquiera de las plataformas para las que esté disponible el producto, durante todo el plazo de garantía, sin sobrecoste adicional.

Se incluye:

- Acceso a los recursos de auto-servicio de las bases de datos de incidencias del fabricante en la modalidad establecida.
- Acceso al portal web de soporte del fabricante.
- Acceso a las nuevas versiones de cualquier componente de la solución cuando estén disponibles. El adjudicatario deberá efectuar la entrega de las nuevas versiones por los medios electrónicos adecuados. Previamente, el adjudicatario entregará una lista de las nuevas funcionalidades de la versión, que incluirán mejoras generales, nuevas funcionalidades y/o correcciones a bugs de la solución.
- Soporte para la puesta en producción de las nuevas versiones y parches del software de cualquier componente de la solución propuesta. Comprende todos los procesos de parametrización, pruebas y validación de las nuevas funcionalidades, en los diferentes entornos afectados. Este soporte deberá llevarse a cabo en todas las instalaciones donde se encuentre implantada la solución objeto de este pliego.
- Los procesos de puesta en producción se deberán ajustar al procedimiento establecido por la DGSD vigente en cada momento.
- El fabricante estará en disposición de recibir comunicaciones de avería o incidencias con una disponibilidad de 24 x 7 x 4 x 365 (24 horas diarias todos los días del año). Este procedimiento contemplará, al menos, la apertura de incidencias por vía telefónica, mail, página web o SMS.
- En el caso de que se produzca una incidencia, el fabricante asignará un Técnico especializado en las soluciones que llevará el caso hasta la completa resolución de la incidencia.
- El fabricante deberá proveer el servicio de garantía en castellano.
- El fabricante realizará informes preventivos sobre el estado de la configuración y los enviará periódicamente. Así mismo, tendrá disponible asesoramiento técnico especializado para revisar las conclusiones de cada informe preventivo y aportar directrices sobre cómo llevarlos a cabo.
- Para los productos software y hardware, la DGSD podrá realizar un número ilimitado de accesos al servicio de apertura de incidencias.
- Para asegurar el cumplimiento del compromiso de tiempo de reparación, el fabricante garantizará un inventario de repuestos críticos.
- Derecho de acceso a un portal de información personalizada del fabricante sobre los equipos, que incluya:
 - Visibilidad instantánea y segura de cualquier alerta que se produzca en la infraestructura.

- Gestión del inventario de activos.
- Monitorización remota 24x7.
- Apertura y seguimiento automático de las incidencias.

La siguiente tabla muestra los niveles de servicios y tiempos máximos obligatorios a cumplir por el fabricante para cualquier tipo de incidencia:

Nivel de gravedad	DESCRIPCIÓN DE LA SEVERIDAD DEL INCIDENTE	Respuesta inicial de Soporte 24x7
Nivel 1	Todas las funciones o una proporción sustancial de las funciones de la infraestructura no están disponibles y no hay una solución provisional posible, o el sistema va tan lento que los tiempos de respuesta lo hacen inutilizable, y/ o hay un problema que ha causado o tiene el potencial de provocar un impacto crítico en el funcionamiento de los servicios de los sistemas de Información.	Dentro de 1 Hora (Cobertura las 24 horas, los siete días de la semana)
Nivel 2	Las funciones o una proporción sustancial de las funciones de la infraestructura no están disponibles y hay una solución provisional posible, o el software ha disminuido su rendimiento de tal forma que los tiempos de respuesta hacen muy difícil su uso y/o hay un problema que causa o tiene potencial de provocar un impacto significativo en los servicios de los sistemas de Información	Dentro de 2 Horas
Nivel 3	Cualquier función del software que no está disponible o el software ha disminuido su rendimiento, o no funciona de la forma documentada, de tal forma que impacta en una reducción de eficiencia que tiene un impacto medio o bajo en los servicios de los sistemas de Información. Una solución provisional puede ser aceptable y se propone e implementa por la empresa adjudicataria.	Dentro de 4 Horas
Nivel 4	Cualquier petición de incremento de funcionalidades que tenga mínimo o ningún impacto en los servicios de los sistemas de Información y para las que no se requiere una solución inmediata. Solicitudes de información o consultas	Dentro de 1 Día Hábil

Los licitadores deberán ofertar los equipamientos bajo una modalidad de garantía del fabricante que dé cuenta de las exigencias contenidas en este apartado.

I.4. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Se suministrarán todas las licencias de software embarcado o adicional para el cumplimiento de todas las funcionalidades y gestión de la plataforma de CIBERRESILIENCIA solicitada en este documento.

Vigencia de las licencias: 4 años

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

Los programas deben 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 una modalidad de licenciamiento de recursos de almacenamiento destinados a la plataforma	• Derecho de uso: por capacidad de almacenamiento de la plataforma Ciberresiliencia suministrada. • Derecho de actualización: Actualización de versiones y configuraciones que resulten por el fabricante. ○ 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 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 realizar un número ilimitado de accesos al servicio de apertura de incidencias • Derecho de consulta al fabricante (soporte del fabricante): ○ Horario: <i>Soporte ininterrumpido 24x7</i> • Derecho de Tratamiento específico para aquellas incidencias con prioridad muy alta.																								
	<table><tr><th rowspan="2">Nivel de gravedad</th><th>1: Crítico</th><th>2: Alto</th><th>3: Medio</th><th>4: Bajo</th></tr><tr><td>El sistema de producción está inactivo</td><td>Fallo de función o característica principal</td><td>Fallo de función o característica menor</td><td>Problema menor</td></tr><tr><td>Descripción del nivel de gravedad</td><td>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.</td><td>Fallo de funcionalidad principal. Las operaciones están muy restringidas, aunque la actividad puede continuar, pero de forma limitada. Existe una solución alternativa temporal.</td><td>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.</td><td>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</td></tr><tr><td colspan="5">Objetivos de tiempos de respuesta</td></tr><tr><td>Asistencia Empresarial, 24*7,</td><td>2 horas</td><td>8 horas</td><td>12 horas</td><td>1 día hábil</td></tr></table>	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					Asistencia Empresarial, 24*7,	2 horas	8 horas	12 horas	1 día hábil
	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																								
	Asistencia Empresarial, 24*7,	2 horas	8 horas	12 horas	1 día hábil																				

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

II.1. SERVICIOS DE INSTALACIÓN AVANZADA DE LOS SUMINISTROS

Alcance

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, traspaso de conocimientos, puesta en servicio de las suscripciones software 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. Incluyendo:
 - Análisis del entorno: Se recolectará toda la información necesaria para reflejar la topología del equipamiento en producción. Se deberá tener en consideración al menos:
 - Arquitectura de la infraestructura de backup existente y arquitectura de datos no estructurado, en las ubicaciones de la DGSD en los sistemas de origen.
 - Diseño de una política de copia de seguridad para la plataforma de información no estructurada que implique el uso de snapshots y la revisión de alojamiento y retención en los repositorios de datos no estructurado y de objetos de la DGSD.
 - Revisión de las versiones de código de los aplicativos de dichas infraestructuras.
 - Listado de servicios IT en coordinación con la DGSD, a incluir en el Vault.
 - Huellas, consumos eléctricos y cableados.
 - Plan de seguridad de acceso a esta plataforma.
 - Planificación de las redes necesarias tanto de uso habitual como de casos excepcionales incluyendo las reglas de FW si fuera necesario.
 - Detalle de las versiones de código suficientes y necesarias para la nueva infraestructura.

- Estrategia de licenciamiento de los servidores de backup /vault en el entorno de Vault teniendo en cuenta que los modelos de licenciamiento actuales productivos de ambos entornos son por capacidad respaldada.
- Instalación física y lógica, de todos los elementos suministrados, configuración 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.

Así mismo, se llevará a cabo una personalización de la infraestructura, para adecuarla al entorno de la DGSD.

Para ello se deberán realizar los siguientes trabajos:

- Se configurará y personalizará tanto la parte del software de automatización de copia de datos al Vault, integrándose con el software productivo de copia de seguridad, así como la parte del software de análisis de comportamiento inusuales.
- Configuración y personalización de la arquitectura para el dato no estructurado definida en diseño.
- Se bastionará el entorno en base a los requisitos de diseño acordados.
- Se establecerán tareas recurrentes de monitorización y de copias, y alertas en caso de patrones sospechosos. Se adecuarán informes para poder revisar que los cambios en la información son los adecuados.
- Pruebas de conexión e integración de los switches a la red de comunicaciones productiva de la DGSD.
- Transferencia y copia inicial de los servicios IT definidos en fase de diseño alojados en los sistemas de backup estructurado al Vault.
- Transferencia y copia inicial de los servicios IT definidos en fase de diseño alojados en los sistemas de datos no estructurados al Vault.
- Pruebas de configuración y administración de los servidores de control y comprobación de la información en el Vault.
 - Se incluirán pruebas de encriptación forzada de documentos y su detección en las copias de seguridad Vault para emular los ciberataques más comunes.
- Pruebas para la puesta en marcha del entorno de recuperación
- Pruebas de restauración del servidor de backup dentro del Vault.
- Pruebas de restauración de información desde el Vault en sistemas de backup habituales o sistemas de producción para datos estructurados en las siguientes tipologías:
 - Máquinas virtuales.
 - Sistemas de ficheros NDMP.
 - Bases de datos Oracle y SQL Server

- Pruebas de restauración de información desde el Vault de los datos no estructurados en los sistemas de backup habituales o en los sistemas de producción de la DGSD para datos no estructurados.

Una vez realizadas las pruebas requeridas en esta fase, la conexión con la red de la DGSD quedará deshabilitada para devolver al Vault a su estado de aislamiento.

- Transferencia de conocimiento al personal de administración de la DGSD del despliegue de la solución y situación final de la plataforma que incluirán los siguientes aspectos:
 - Administración de todos los equipos hardware adquiridos.
 - Personalización y administración de la plataforma de Ciberresiliencia con especial hincapié en:
 - Procedimientos de supervisión y control de la modificación de la información de copia de seguridad.
 - Procedimientos de restauración rápida o exhaustiva desde el Vault a Sistemas en Producción.
 - Tareas de mantenimiento de la configuración y supervisiones periódicas.
 - Monitorización de todos los elementos del entorno Vault.
 - Detección de problemas habituales y posibles reparaciones.

En cuanto a las transferencias de conocimiento, podrán impartirse a lo largo del proyecto sin tener que coincidir en un punto en el tiempo. El objetivo principal será que el personal que administra y opera la plataforma sea capaz de conocer el sistema implantado en profundidad, y así efectuar la correcta realización de los trabajos, la revisión integral de los equipos y la localización y reparación de averías.

Así, pues, las características de estas transferencias de información serán las siguientes:

- Deberá ser una transferencia de información personalizada, referida exclusivamente al entorno implantado en la DGSD y su contenido será exclusivamente referido a este.
- Será planificado y/o impartido por el arquitecto de la solución y en él se harán las simulaciones necesarias para comprender y comprobar el correcto funcionamiento de la solución.
- Características generales y plan de trabajo: Se solicita una transferencia de información práctica. Los usuarios de esta transferencia de conocimientos serán los administradores de la plataforma.
- Lugar de Impartición: mientras la plataforma no haya entrado en producción se podrán dar online, pero una vez que haya entrado en producción se deberán impartir de forma presencial en las instalaciones de la DGSD debido al

aislamiento de la plataforma, excepto que la situación sanitaria lo impida convenientemente.

- Materiales: Se entregará una copia electrónica del material del curso a cada uno de los participantes.

El alcance de las transferencias de conocimiento deberá incluir:

- Administración de los diferentes productos, recorrido completo por las opciones de configuración, consolas disponibles en función de los roles y capacidades, etc.
 - Métodos de desarrollo de funcionalidades avanzadas, scripts, flujos de acciones, etc.
 - Capacidades de integración con las tecnologías de comunicaciones existentes en la DGSD.
 - Respuesta ante incidencias de la Plataforma.
 - Análisis de rendimiento.
 - Pruebas de restauración.
- Entrega de Documentación.
 - Manuales y procedimientos de administración del entorno.
 - Manuales y procedimientos de operación de la nueva Plataforma: guía detallada de monitorización.

Las ofertas desglosaran el importe correspondiente a la instalación avanzada.

Hitos y entregables

Hito	Descripción del hito y sus entregables	Plazo	Porcentaje de la prestación
HITO_01	Descripción del hito: Diseño de la implantación de los productos adaptados a los requisitos tecnológicos de la DGSD Entregables: Documentos de Diseño Alto nivel y Bajo Nivel	2 meses a partir del inicio de la ejecución	35%
HITO_02	Descripción del hito: Instalación física y lógica, de todos los elementos suministrados, configuración 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. Entregables: ● Documento de instalación. ● Cuaderno de pruebas u otras evidencias de que se han realizado las tareas	4 meses después de la aceptación del HITO_01	50%

HITO_03	Descripción del hito: transferencia de conocimiento al personal de administración de la DGSD del despliegue de la solución y situación final de la plataforma. Entregables: • Documento de situación final de la plataforma. • Documentos de guías de Administración. • Manuales y procedimientos de operación de la nueva Plataforma: guía detallada de monitorización.	1 mes después de la aceptación del HITO_02	15%
---------	--	--	-----

En cuanto a la gestión, supervisión y dirección de los trabajos, la empresa adjudicataria designará un interlocutor del servicio quien mantendrá la necesaria y permanente coordinación con el grupo Responsable designado por la DGSD, cuya función principal será la interlocución con el Contratista en lo que respecta a la ejecución del servicio y a la gestión y supervisión del mismo; así como, la recepción y aceptación final de los diferentes productos entregables, y la gestión de cualquier aspecto del contrato que requiera un análisis.

El Contratista dentro de la gestión del proyecto realizará al menos las siguientes labores:

- Comunicación activa y directa con el grupo responsable designado por la DGSD.
- Entrega de manera periódica un resumen con los avances del proyecto, situación actual, posibles riesgos. Dicho periodo de entrega será acordado por el grupo responsable designado por DGSD.
- Realización de reuniones periódicas de seguimiento.
- Realización de actas de las reuniones que tengan lugar a lo largo de todo el proyecto.
- Se responsabilizará de la efectiva entrega de la documentación a entregar a DGSD en cualquiera de los ámbitos del proyecto.

II.2. SERVICIOS DE SOPORTE DE LOS SUMINISTROS

NO APLICA

II.3. REQUISITOS DE LOS PERFILES PROFESIONALES

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

ANEXO III TRATAMIENTOS DE DATOS, FINALIDAD Y MEDIDAS

III.1. TRATAMIENTOS DE DATOS Y FINALIDAD DE LOS TRATAMIENTOS

Si en el apartado 2.3. se ha indicado que existe tratamiento de datos personales, a continuación, se señalan los datos personales que se van a transmitir y almacenar en la nube objeto del suministro:

- Categorías de interesados cuyos datos personales se tratan: Haga clic o pulse aquí para escribir texto.
- Categorías de datos personales tratados: Haga clic o pulse aquí para escribir texto.
- Datos sensibles tratados (si procede) y restricciones o garantías aplicables: Haga clic o pulse aquí para escribir texto.
- Naturaleza del tratamiento: Haga clic o pulse aquí para escribir texto.
- Finalidad(es) del tratamiento: Haga clic o pulse aquí para escribir texto.
- Duración del tratamiento: Haga clic o pulse aquí para escribir texto.

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

III.2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Serán de aplicación las medidas técnicas y organizativas para garantizar la seguridad de los datos, 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 IV ENTREGAS PARCIALES

NO APLICA

ANEXO V COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO

NO APLICA

ANEXO VI 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 24/2021; Expediente 2022/68), 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.⁹
- **Certificación positiva** de la Agencia Estatal de Administración Tributaria de hallarse los subcontratistas al corriente en el cumplimiento de las obligaciones tributarias o, alternatively, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.
- **Certificación positiva** de la Tesorería General de la Seguridad Social de hallarse los subcontratistas al corriente de sus obligaciones con la Seguridad Social o, alternatively, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a de de

Firmado electrónicamente

⁹ La declaración responsable deberá formularse en los siguientes términos “Que ni el firmante de la declaración, ni la persona física/jurídica a la que representa, ni ninguno de sus administradores o representantes se hallan incurso en supuesto alguno a los que se refiere el artículo 71 de la LCSP.”

ANEXO VII

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

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

Efectúa las siguientes **DECLARACIONES**

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

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

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

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

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

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

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

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

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

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

Acredita la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT (declaración censal 036 o 037¹⁰ o documento equivalente de las Administraciones Forales) que incluye la actividad objeto del contrato basado conforme a lo previsto en el artículo 8 apartado 2 de la Orden HFP/1030/2021, de 29 de septiembre).

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

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

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

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

....., XX de de 202X
Fdo.
Cargo:

¹⁰ Estas declaraciones podrán obtenerse por las empresas en la sede de la AEAT en el siguiente enlace <https://sede.agenciatributaria.gob.es/Sede/tramitacion/G322.shtml> . Si tienen dudas llamen al teléfono general de consultas de la Agencia Tributaria o al 060.

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

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

En todos los contratos específicos financiados¹¹ por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiables, estableciéndose las siguientes **obligaciones**:

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

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

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

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

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

Los participantes en el procedimiento deben cumplimentar la declaración de ausencia de conflicto de interés (DACI) en los términos previstos en los planes de medidas antifraude y

¹¹ O es susceptible de ser financiado en caso de no haberse aún confirmado la selección por las autoridades correspondientes.

anticorrupción. En los contratos sujetos al PRTR, las medidas serán conformes con las disposiciones de la Orden HFP/1030/2021.

5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

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

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

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

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

7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

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

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

8. PROHIBICIÓN DE DOBLE FINANCIACIÓN

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

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

1. RÉGIMEN JURÍDICO APLICABLE

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

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

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

El contrato se enmarca en el **Componente C11. Inversión I3**
Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y las Entidades Locales

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

Etiquetado verde	Etiquetado digital
	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:

Según el Anexo VII 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, donde se especifica la metodología para el etiquetado digital, el tipo de intervención aplicable es el 011: Soluciones de TIC para la Administración, servicios electrónicos, aplicaciones, cuyo coeficiente es el 100%.

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>Servidores y sistemas de almacenamiento</i>	<i>Mitigación cambio climático Transición a una economía circular</i>	<i>Los equipos que se utilicen cumplirán los requisitos relacionados con el consumo energético establecidos de acuerdo con la Directiva 2009/125/EC</i>
<i>Servidores y sistemas de almacenamiento</i>	<i>Transición a una economía circular</i>	<i>Los equipos no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE.</i>

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

() Otras penalidades

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

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

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

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

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

- 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).