

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

(Expediente nº 2022/48)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

**SOFTWARE DE AUDITORÍA Y ADMINISTRACIÓN DE
SERVIDORES WINDOWS. EXP. 236/2025**

Lote 2 - Software para la gestión de infraestructura

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

TÉRMINOS Y CONDICIONES

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

12.	PENALIDADES	20
12.1.	Penalidades fijadas en el sistema dinámico de adquisición	20
12.2.	Fórmula para la aplicación de penalidades	21
13.	CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO.....	22
14.	FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS	22
	ANEXO I PRESCRIPCIONES TÉCNICAS	25
I.1.	Requisitos funcionales de los programas a suministrar	25
I.2.	Requisitos no funcionales de los programas a suministrar	40
I.3.	Periodo de vigencia y modalidad de licenciamiento	41
I.4.	Requisitos de seguridad de los programas en la nube	42
	ANEXO II SERVICIOS DE INSTALACIÓN AVANZADA Y/O SOPORTE A PROPORCIONAR POR EL ADJUDICATARIO	42
II.1.	Servicios de instalación avanzada de los programas a suministrar	42
II.2.	Servicios de soporte de los programas a suministrar	44
II.2.1.	Dimensionamiento del servicio.....	45
II.2.2.	Acuerdos de nivel de servicio.....	45
II.3.	Requisitos de los perfiles profesionales	46
	ANEXO III TRATAMIENTOS DE DATOS EN LA NUBE, FINALIDAD Y MEDIDAS	47
III.1.	Tratamientos de datos y finalidad de los tratamientos	47
III.2.	Medidas técnicas y organizativas.....	47
	ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE	50
	ANEXO V MODELO DE DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	51
	ANEXO VI Manifestación de conformidad del responsable del tratamiento DE LOS DATOS DEL ORGANISMO DESTINATARIO	53
	ANEXO VII ENTREGAS PARCIALES.....	54
	ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO	55
	ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN	56
	ANEXO X DECLARACIÓN MÚLTIPLE DE LAS EMPRESAS PROPUESTAS COMO ADJUDICATARIAS DE CONTRATOS ESPECÍFICOS CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA	¡Error! Marcador no definido.
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	¡Error! Marcador no definido.
a.	Obligaciones generales aplicables a todos los contratos financiados con cargo al presupuesto de la Unión Europea	¡Error! Marcador no definido.
b.	Obligaciones generales aplicables a los contratos financiados con cargo al PRTR	¡Error! Marcador no definido.

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

Organismo destinatario

Unidad proponente: : Área de Infraestructura Informática

Centro directivo: Dirección de Innovación e Ingeniería

Departamento/organismo: Canal de Isabel II, S.A., M.P.

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

Elías Manrique Rojo – Jefe de Área de Infraestructura Informática, dependiente orgánicamente de la Subdirección de Sistemas Informáticos y de la Dirección de Innovación e Ingeniería de Canal de Isabel II S.A. M.P.

Datos de contacto:

Dirección Postal: Calle Santa Engracia 125, Edificio 4 – 28003 Madrid

Correo electrónico: emanrique@canal.madrid

Teléfono: 915451291

Órgano de Contratación:

El órgano de contratación competente para la adjudicación del contrato es el Consejero Delegado de Canal de Isabel II, S.A., M.P.

2. LOTE, TÍTULO Y OBJETO DEL CONTRATO ESPECÍFICO

2.1. LOTE, TÍTULO Y OBJETO

Lote objeto de licitación: Lote 2 - Software para la gestión de infraestructura

Título del contrato: Software de auditoría y administración de servidores Windows. Exp. 236/2025

Objeto del contrato:

El objeto del contrato es la adquisición de software de sistema orientado a la auditoría y administración de servidores con sistema operativo Windows Server, su mantenimiento y soporte durante un periodo de 3 años.

La solución propuesta puede ser una única herramienta que cumpla con todos los requisitos funcionales y especificaciones técnicas solicitados, o un conjunto de herramientas del mismo fabricante que estén integradas entre sí y cumplan con dichos requisitos y especificaciones. Conjuntamente con la solución ofertada se solicita una asistencia técnica para la configuración y puesta en marcha de las herramientas.

2.2. CARACTERÍSTICAS PRINCIPALES DE LAS PRESTACIONES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Relación de los suministros con la arquitectura de seguridad

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

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

Haga clic o pulse aquí para escribir texto.

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

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

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

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

☐ Los programas objeto del suministro deben procesar o almacenar datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, conforme a lo dispuesto en la **Directiva (UE) 2016/680** y la **Ley Orgánica 7/2021**. Se describen las condiciones aplicables en el apartado 9.4 de este documento de invitación.

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

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

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

3. DURACIÓN DEL CONTRATO

3.1. FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

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

3.2. PLAZO DE ENTREGA DE LAS LICENCIAS

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

3.3. PLAZO DE EJECUCIÓN DEL CONTRATO

- ☒ Se requiere la instalación y configuración básica de las licencias, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo⁴ de 30 días hábiles, incluido el plazo de entrega de las licencias.
- ☒ El contrato incluye el servicio de instalación avanzada, a prestar por el adjudicatario, descrito en el **Anexo II** apartado 1. El plazo de ejecución de este servicio incluye el plazo para la entrega de las licencias y para la instalación y configuración básica.
 - Plazo de ejecución: 45 días
- ☒ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario, descritos en el **Anexo II**, apartado 2:
 - Plazo de ejecución (señalar únicamente una opción):
 - ☒ 36 meses a contar desde el final de la instalación básica y, en su caso, de la instalación avanzada.
 - ☐ Hasta la expiración de la vigencia de las licencias objeto del suministro.

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

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

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

3.4. PRÓRROGA DEL CONTRATO ESPECÍFICO

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

4. VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN

4.1. PRESUPUESTO DE LICITACIÓN Y APLICACIONES PRESUPUESTARIAS

Presupuesto total sin impuestos (€)	Impuestos indirectos (€)	Presupuesto total con impuestos (€)
156.000,00 €	32.760,00 €	188.760,00 €

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	Impuestos indirectos (€)	Presupuesto con impuestos (€)
SUMINISTRO			
Suministro de licencias (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	150.023,87 €	31.505,01 €	181.528,88 €
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	3.984,09 €	836,66 €	4.820,75 €
Servicio de soporte, a prestar por el adjudicatario	1.992,04	418,33€	2.410,37
TOTAL	156.000,00 €	32.760,00 €	188.760,00 €

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

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

Las obligaciones económicas que se deriven para la Administración por el cumplimiento del contrato serán financiadas por el Presupuesto de Gastos del organismo Canal de Isabel II, S.A.,

M.P., Centro de Gestión U164000 – Área de Infraestructura Informática, con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	Anualidad 2025 (IVA incluido)	Anualidad 2026 (IVA incluido)	Anualidad 2027 (IVA incluido)	Anualidad 2028 (IVA incluido)	TOTAL (IVA incluido)
U164000	0	186.340	1.210	1.210	188.760

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	5.021,96 €
Resto costes directos	150.023,87 €
Costes indirectos + Gastos generales + Beneficio industrial	954,17 €
Total sin IVA	156.000,00 €

Justificación: El cálculo del valor estimado del contrato se ha realizado teniendo en cuenta precios de mercado de varias soluciones de auditoría y administración de servidores Windows y Active Directory. A tal efecto, Canal de Isabel II, S.A., M.P. ha solicitado demostraciones prácticas de varias soluciones de mercado y calculado el presupuesto para su parque de servidores Windows en los configuradores online de fabricantes o solicitando presupuestos tras las demostraciones.

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

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

El convenio colectivo sectorial de aplicación en los términos indicados es el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública, publicado en el BOE del día 16 de abril de 2025 mediante Resolución de 4 de abril de 2025, de la Dirección General de Trabajo, por la que se registra y

publica el citado Convenio. No consta que exista diferencia por género en el Convenio colectivo que resulta de aplicación.

Aplicando al coste de personal del año 2.026 según convenio los coeficientes estándar de gastos generales del 13% y de beneficio industrial del 6%, da un precio por esos servicios es de 5.976,13 €. correspondientes a 30 días de ejecución del proyecto de instalación avanzada y 15 días de soporte y mantenimiento durante la vigencia del contrato.

<i>Costes de personal</i>							
<i>Perfiles</i>	<i>Dedicación</i>	<i>Salario Base</i>	<i>Especialización tecnológica (XX%)</i>	<i>Salario anual</i>	<i>Coste anual según dedicación</i>	<i>Coste personal contrato</i>	<i>Coste personal contrato con Seguridad Social 30%</i>
Administrador de sistemas Área 3 – Grupo A1	12,50% (1 mes y medio)	28.430,27	-	30.904,37	3.863,04	3.863,04	5.021,96

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:

Se aplicarán los precios unitarios ofertados para el modo de licenciamiento que requiera la ampliación de licencias por las circunstancias señaladas a continuación.

- Circunstancias admitidas para modificar el contrato específico⁵:
 - Incremento de la necesidad de licencias/suscripciones debido al incremento del número de servidores a gestionar.

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

- Incremento de la necesidad de licencias/suscripciones debido al incremento número de técnicos que hacen uso de las mismas.

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 **CIENTO OCHENTA Y SEIS MIL EUROS euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	156.000,00 €
Importe máximo por modificación prevista, sin IVA	30.000,00 €
TOTAL	186.000,00€

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

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

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

- ☒ No.
- ☐ Sí. Instrumento /Fondo/Programa/Mecanismo: Haga clic o pulse aquí para escribir texto.
- Código de operación/Proyecto/Iniciativa: Haga clic o pulse aquí para escribir texto.

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

5. LUGAR Y CONDICIONES DE LA ENTREGA

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

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

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

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

6. INCOMPATIBILIDADES PARA LA LICITACIÓN

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

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

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

☐ Otras:
(*Detallar en su caso*)

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

7. CRITERIOS DE VALORACIÓN DE LAS OFERTAS Y SU PONDERACIÓN⁶

7.1. PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN

☐ El único criterio de adjudicación es el precio

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

SOBRE 1.1 Criterios evaluables mediante fórmulas distintos al precio	SOBRE 1.2. Precio
50 puntos	50 puntos

☐ 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.	Haga clic o pulse aquí para escribir texto.	Haga clic o pulse aquí para escribir texto.

7.2. FÓRMULA APLICABLE AL CRITERIO PRECIO

☐ Función **optimizar precio** (si se incluyen criterios cuya cuantificación depende de un juicio de valor, se deberá usar ésta obligatoriamente):

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

Donde:

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

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

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

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

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

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

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

Donde:

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

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

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

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

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

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

7.3.1. CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS

CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓN, según apartado 7.5
Cumplimiento de "Requisitos de auditoría y gestión de Active Directory".	10	Sí/No

Cumplimiento de los criterios cuantificables del apartado 1 “Requisitos de auditoría y gestión de Active Directory”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 1 punto.		
Cumplimiento de “Requisitos de auditoría y gestión sobre Azure EntraID”. Cumplimiento de los criterios cuantificables del apartado 2 “Requisitos de auditoría y gestión sobre Azure EntraID”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 1 punto.	4	Sí/No
Cumplimiento de “Requisitos de auditoría y gestión de servidores Windows”. Cumplimiento de los criterios cuantificables del apartado 3 “Requisitos de auditoría y gestión de servidores Windows”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 1 punto.	4	Sí/No
Cumplimiento de “Requisitos de auditoría de sistemas de ficheros (Servidores de ficheros Windows, cabinas NetApp, Nutanix Files y Azure File Shares). Cumplimiento de los criterios cuantificables del apartado 4 “Requisitos de auditoría de sistemas de ficheros”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 1 punto.	4	Sí/No
Cumplimiento de “Requisitos de gestión de accesos privilegiados PAM”. Cumplimiento de los criterios cuantificables del apartado 5 “Requisitos de gestión de accesos privilegiados PAM”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 4 puntos.	20	Sí/No
Cumplimiento de “Requisitos de gestión de parches y actualizaciones Windows”. Cumplimiento de los criterios cuantificables del apartado 6 “Requisitos de gestión de parches y actualizaciones Windows”. El cumplimiento de cada requisito considerado como criterio cuantificable se valorará con 2 puntos.	6	Sí/No
Software ofertado en modo licencia perpetua	2	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**:

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

Donde:

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

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

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

$$X_i = P$$

Donde:

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

7.4. CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR

7.4.1. CRITERIOS Y PONDERACIÓN

CRITERIO	PUNTOS
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: Haga clic o pulse aquí para escribir texto..
 - ☒ 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 %.

Haga clic o pulse aquí para escribir texto.

9. CONDICIONES DE EJECUCIÓN Y OTRAS OBLIGACIONES DEL CONTRATISTA

9.1. OBLIGACIONES GENERALES

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

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

No hay tareas críticas.

- h) Si el contrato incluye servicios a prestar por el adjudicatario, estará obligado al cumplimiento de las condiciones salariales de los trabajadores conforme al convenio colectivo sectorial de aplicación conforme al artículo 122.2 de la LCSP.
- i) El adjudicatario nombrará un Coordinador Técnico del Contrato que actuará como interlocutor único a todos los efectos frente a la entidad destinataria del contrato, canalizando las comunicaciones y responsabilizándose de la gestión de la prestación por parte de la empresa adjudicataria.

9.2. OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO

No aplica.

9.3. OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

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

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

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

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

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

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

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

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

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

10. PAGO Y FACTURACIÓN

10.1. PAGO DEL PRECIO

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

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

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

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

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

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

Período 3: Haga clic o pulse aquí para escribir texto.

Período 4: Haga clic o pulse aquí para escribir texto.

☒ Otra: Anualmente.

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

☒ Organismo adherido al Sistema Estatal de Contratación Centralizada.

Las facturas se presentarán obligatoriamente en formato electrónico firmadas con firma electrónica avanzada basada en un certificado reconocido.

La facturación de las licencias y del servicio de instalación avanzada se realizará a la recepción de dicho servicio de instalación avanzada.

La facturación del soporte se realizará anualmente, pudiendo el primer pago realizarse conjuntamente con la factura de licencias y servicio de instalación avanzada.

11. GARANTÍA DE LOS BIENES

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

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

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

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

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

12. PENALIDADES

12.1. PENALIDADES FIJADAS EN EL SISTEMA DINÁMICO DE ADQUISICIÓN

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

	Valor fijado en el SDA	Valor fijado en el contrato específico	Fórmula de cálculo
Incumplimiento de las condiciones especiales de ejecución, excepto las relativas a subcontratación. <i>Si fuera necesario, detallar los supuestos de ejecución defectuosa:</i> - ... - ...	2% de la facturación del periodo		Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo		<i>Según ANS.</i>
Incumplimiento de los compromisos de adscripción de medios.	2% de la facturación del periodo		Apartado 12.2
Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas.	2% de la facturación del periodo	Grave: hasta el 5% del importe del contrato Muy grave: hasta el 10% del importe del contrato	Apartado 12.2
Demora en el cumplimiento del plazo total del contrato	Resolución / 0,60 euros por cada día y 1.000 euros del precio del contrato, IVA excluido		Valor fijado en el SDA
Incumplimiento de obligaciones en materia medioambiental, social o laboral	2% de la facturación del periodo		Apartado 12.2

Incumplimiento de las condiciones de subcontratación	2% del importe del subcontrato	Valor fijado en el SDA
Incumplimiento de las obligaciones de información y pago sobre suministradores y subcontratistas.	2% del importe del subcontrato	Valor fijado en el SDA

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

- El incumplimiento de las medidas relativas a la seguridad de los programas en cumplimiento del ENS, o de los requisitos de seguridad para la protección de datos personales en nube tendrá la consideración de incumplimiento **muy grave** dando lugar a una penalidad de hasta el **10% del importe total del contrato**.
- Incumplimiento del resto de las condiciones especiales de ejecución
 - Grave:
 - Muy grave:
- Incumplimiento de los ANS:
 - Grave:
 - Muy grave:
- Incumplimiento de los compromisos de adscripción de medios
 - Grave:
 - Muy grave:
- Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas
 - Grave: La falta de adecuación o incumplimiento de 1 o 2 requisitos funcionales que se hubieran justificado y aceptado en la valoración de los criterios tendrá la consideración de incumplimiento grave y una penalización del 5% del importe del contrato
 - Muy grave: La falta de adecuación o incumplimiento de 3 o más requisitos funcionales que se hubieran justificado y aceptado en la valoración de los criterios tendrá la consideración de incumplimiento Muy Grave y una penalización del 10% del importe del contrato.

12.2. FÓRMULA PARA LA APLICACIÓN DE PENALIDADES

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

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

Donde:

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

13. CAUSAS DE RESOLUCIÓN DEL CONTRATO ESPECÍFICO

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

Haga clic o pulse aquí para escribir texto.

14. FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS

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

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

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

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

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

La oferta técnica deberá contener la siguiente documentación:

- Relación de los programas en la modalidad de licenciamiento que se ofertan
- La información de los requisitos mínimos de los productos o referencias a las fichas técnicas o catálogos que permitan acreditar los criterios automáticos:
 - *Incluir relación de requisitos o referencia a Anexo para cumplimentación por parte de los licitadores*
- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - *Incluir relación de requisitos o referencia a Anexo para cumplimentación por parte de los licitadores*
- Si la oferta incluye programas que forman parte de la arquitectura de seguridad del organismo **se deberá incluir la acreditación de los requisitos de seguridad** exigidos por cualquiera de los medios descritos en el apartado III.2.2 o III.2.3 del PPT, según corresponda. La falta de acreditación será motivo de exclusión de la oferta.

⁸ Plataforma de Contratación del Sector Público: <https://contrataciondelestado.es/wps/portal/quiasAyuda>

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

En el supuesto de que se hayan definido criterios sujetos a juicio de valor, se deberá incluir en el Sobre 1 de la oferta técnica, la documentación que permita evaluar los planes de implantación o las soluciones técnicas conforme a los criterios sujetos a un juicio de valor, sin que sea posible incluir en este sobre información económica o correspondiente a criterios automáticos que se presentará en el Sobre 2. El Sobre 1 se deberá valorar de forma previa a la apertura del sobre que contiene la documentación económica y de los criterios evaluables mediante fórmulas.

Las proposiciones se presentarán a través del **Sistema Licit@ (sistema de licitación electrónica de la Comunidad de Madrid)** en el plazo y antes de la hora que se determine en el correspondiente anuncio de licitación.

En el Portal de la Contratación Pública de la Comunidad de Madrid (<https://contratos-publicos.comunidad.madrid/perfil-contratante/sistema-licit-licitacion-electronica>) se ofrece la información necesaria y el acceso al Sistema Licit@ que debe utilizarse, así como el formulario para solicitar ayuda al equipo de soporte del sistema ante eventuales incidencias técnicas (este es el único cauce habilitado para resolver dichas incidencias). En cualquier caso, se recomienda realizar la presentación de la oferta con antelación suficiente para solucionar eventuales incidencias.

Para la aportación de documentos los licitadores deberán usar el Servicio de aportación de documentos de la Sede Electrónica de la Comunidad de Madrid (<https://sede.comunidad.madrid/guia-tramitacion-electronica#documentos>).

Los licitadores podrán plantear consultas sobre el presente procedimiento de licitación a través de la dirección: consultas_contratacion@canal.madrid hasta cuatro días antes del límite de presentación de ofertas de la presente licitación.

Las ofertas deberán incluir la siguiente documentación:

- Relación de los programas junto con la modalidad de licenciamiento que se ofertan.
- Anexo X modelo de proposición económica cumplimentada y firmada por el licitador.
- Anexo XII Acreditación requisitos obligatorios y acreditación de los requisitos considerados como criterios cuantificables y la documentación acreditativa referida en el Anexo XI.

Haga clic o pulse aquí para escribir texto.

- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
 - No aplicaSi la oferta incluye programas que forman parte de la arquitectura de seguridad del organismo **se deberá incluir la acreditación de los requisitos de seguridad** exigidos por cualquiera de los medios descritos en el apartado III.2.2 o III.2.3 del PPT, según corresponda. La falta de acreditación será motivo de exclusión de la oferta.

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, PREVALECERÁN ESTOS ÚLTIMOS.

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

EL TITULAR DEL ÓRGANO DESTINATARIO (CARGO): Consejero Delegado

Firmado electrónicamente (nombre y apellidos): Mariano González Sáez

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS PROGRAMAS A SUMINISTRAR

El software a suministrar debe cubrir las funcionalidades que se detallan a continuación, cubriendo las necesidades en los siguientes ámbitos:

- Auditoría y gestión del Active Directory on-prem
- Auditoría y gestión del Azure Active Directory (Entra ID)
- Auditoría y gestión de servidores con sistema operativo Windows Server
- Auditoría y gestión de sistemas de ficheros locales, cabinas NetApp, Nutanix y Azure
- Gestión de accesos privilegiados (PAM)
- Gestión y distribución de parches y actualizaciones Windows.

A continuación, se establecen todos los requisitos de la herramienta y éstos se dividen en requisitos obligatorios y requisitos criterios cuantificables.

El cumplimiento de los requisitos obligatorios de la herramienta deberá ser acreditarlos por los licitadores conforme a lo establecido en el Anexo XI aportando el Anexo XII cumplimentado y la documentación acreditativa referida en el Anexo XI. No se tendrá en cuenta la oferta del licitador que no acredite el cumplimiento los requisitos obligatorios.

Los requisitos que se establecen como criterios cuantificables no son obligatorios, pero sí son valorables mediante fórmulas conforme a lo establecido en el apartado 7.3.1 del documento de invitación. En este sentido, para que los licitadores puedan obtener la valoración indicada en el apartado referido anteriormente los licitadores deberán acreditar su cumplimiento conforme a lo establecido en el Anexo XI aportando el Anexo XII y aportando la documentación acreditativa referida en el Anexo XI. En caso contrario se otorgaría 0 puntos a los licitadores que no acrediten los requisitos establecidos como criterios cuantificables

1. Requisitos de auditoría y gestión de Active Directory

1.1. Auditoría de cambios en configuraciones de GPO

- 1.1.1. Generar información detallada sobre GPOs creadas, eliminadas y modificadas, con historial completo de cambios.
- 1.1.2. Auditar e informar sobre cambios en la configuración de GPO con valores antes y después en tiempo real.
- 1.1.3. Informe de historial detallado de cada modificación en las configuraciones de GPO.
- 1.1.4. Mantener historial de auditoría de todas las modificaciones en GPOs para análisis forense y cumplimiento normativo.
- 1.1.5. Registrar en tiempo real los cambios en configuraciones de Windows aplicadas a los usuarios.

- 1.1.6. Enviar notificaciones inmediatas sobre cambios no autorizados en políticas de grupo.
- 1.1.7. Programar informes periódicos sobre la vinculación de GPOs a diferentes niveles (dominio, OU).
- 1.1.8. Generar informes sobre cambios en la configuración de equipos, configuración de usuarios, políticas de contraseñas y políticas de bloqueo de cuentas.
- 1.1.9. Supervisar cambios en configuraciones de seguridad, plantillas administrativas y asignaciones de derechos de usuario.
- 1.1.10. Rastrear modificaciones en configuraciones de Windows, permisos de políticas de grupo y preferencias de políticas de grupo.
- 1.1.11. Informe de GPOs recientemente creados, eliminados y modificados con detalles sobre quién realizó los cambios y cuándo.
- 1.1.12. Monitorizar cambios en enlaces de GPO para asegurar que las políticas se apliquen correctamente.

1.2. Auditoría de Cambios en OUs

- 1.2.1. Detectar la creación, eliminación, movimiento, modificación y restauración de OUs.
- 1.2.2. Rastrear cambios en atributos de OUs, incluyendo listas de control de acceso (ACLs) y atributos extendidos.
- 1.2.3. Visualizar historial completo de OUs para un seguimiento detallado de modificaciones a lo largo del tiempo.
- 1.2.4. Configurar alertas para cambios no autorizados o sospechosos en OUs.

1.3. Auditoría de Cambios en Membresía de Grupos

- 1.3.1. Detectar la inclusión y eliminación de miembros en grupos de seguridad y distribución.
- 1.3.2. Rastrear cambios en atributos de grupos, incluyendo tipo y ámbito.
- 1.3.3. Monitorizar la creación, eliminación, renombrado y movimiento de grupos.
- 1.3.4. Mantener un historial detallado de modificaciones en objetos de grupo, especialmente en grupos privilegiados y sensibles.

1.4. Auditoría híbrida con Azure

- 1.4.1. Supervisar intentos de autenticación y patrones de inicio de sesión en entornos locales y en la nube desde una única consola.

- 1.4.2.Rastrear intentos de establecimiento y restablecimiento de contraseñas en cuentas privilegiadas de Azure.
- 1.4.3.Controlar el acceso mediante la asignación y eliminación de roles en Azure.
- 1.4.4.Alertar a administradores cuando nuevos usuarios sean añadidos o eliminados de grupos en Azure.
- 1.4.5.Monitorizar la gestión de dispositivos BYOD mediante auditorías de cambios en propietarios y usuarios de dispositivos. **CRITERIO CUANTIFICABLE.**
- 1.4.6.Verificar la adición o eliminación de permisos OAuth para proteger aplicaciones en la nube. **CRITERIO CUANTIFICABLE.**

1.5. Auditoría del comportamiento de inicio de sesión de usuarios

- 1.5.1.Obtener un historial de auditoría completo de inicios de sesión, con detalles de quién inició sesión, desde dónde y por cuánto tiempo.
- 1.5.2.Monitorizar y analizar diferentes tipos de inicio de sesión: interactivo, remoto, local y en red.
- 1.5.3.Seguimiento de duración de sesión y tiempo inactivo por usuario.
- 1.5.4.Alertar a los administradores sobre comportamientos atípicos de inicio de sesión, como horarios inusuales.
- 1.5.5.Analizar intentos de inicio de sesión fallidos por nombre de usuario, dirección IP, hora de inicio, motivo (nombre de usuario incorrecto, contraseña incorrecta, contraseña expirada, usuario deshabilitado, restricción horaria, etc.) y otros factores para detectar posibles amenazas.
- 1.5.6.Generar informes sobre tiempos de inicio y apagado de computadoras, horas activas, tipos de apagado, etc.
- 1.5.7.Rastrear el historial y patrones de inicio de sesión de los usuarios para garantizar seguridad y cumplimiento normativo.
- 1.5.8.Supervisar actividades de inicio de sesión RADIUS en equipos remotos. **CRITERIO CUANTIFICABLE.**

1.6. Análisis y resolución de bloqueos de cuentas

- 1.6.1.Auditar y generar informes de cada bloqueo de cuenta con detalles como hora del bloqueo, equipo afectado e historial de inicio de sesión del usuario.
- 1.6.2.Auditar y reportar todos los eventos de desbloqueo de cuentas con detalles como hora del desbloqueo, usuario que desbloquea y equipo desde el que lo hace.

- 1.6.3. Diagnosticar y resolver bloqueos repetidos analizando componentes de Windows como servicios, aplicaciones y tareas programadas.
- 1.6.4. Identificar credenciales obsoletas o mapeos de red defectuosos que causen bloqueos de cuenta.
- 1.6.5. Notificar a los administradores de sistemas cuando cuentas administrativas sean bloqueadas.
- 1.6.6. Detectar ataques de fuerza bruta y responder automáticamente desconectando la sesión del usuario o apagando el sistema comprometido. CRITERIO CUANTIFICABLE.
- 1.6.7. Registrar cuentas frecuentemente bloqueadas para identificar empleados más afectados y analizar las causas de los bloqueos.
- 1.6.8. Detectar y diagnosticar bloqueos de cuentas de AD identificando su causa raíz.
- 1.6.9. Diagnosticar bloqueos de cuentas y detectar credenciales obsoletas, aplicaciones o servicios problemáticos.
- 1.6.10. Generar notificaciones instantáneas cuando se bloquean cuentas de usuario críticas, incluyendo detalles como la hora del bloqueo y la máquina involucrada.
- 1.6.11. Restaurar operaciones localizando cuentas bloqueadas en AD debido a asignaciones incorrectas de unidades de red o sesiones de escritorio remoto desconectadas.
- 1.6.12. Supervisar y reportar todos los bloqueos de AD para cumplir con normativas HIPAA, PCI DSS, SOX.

1.7. Monitorización de Usuarios con Privilegios

- 1.7.1. Supervisar e informar sobre acciones críticas realizadas por administradores o cuentas y grupos con privilegios elevados.
- 1.7.2. Auditar el uso de privilegios en todo el dominio, incluyendo cambios administrativos en el esquema de AD, usuarios, grupos y OUs.
- 1.7.3. Rastrear el acceso de usuarios privilegiados a datos críticos para detectar cambios indebidos o maliciosos.
- 1.7.4. Garantizar el cumplimiento normativo rastreando el acceso de usuarios privilegiados a datos regulados.
- 1.7.5. Identificar intentos de escalado de privilegios con alertas en el primer uso de privilegios elevados.
- 1.7.6. Alertar sobre actividades sospechosas, como el borrado de registros de auditoría o accesos no autorizados fuera del horario laboral.

1.8. Monitorización, auditoría de cambios e informes sobre Windows LAPS.

1.8.1. Auditar y reportar usuarios que consultan passwords

1.8.2. Auditar y reportar usuarios que modifican validez de los passwords

1.9. Detección proactiva de amenazas con Análisis de Comportamiento del Usuario (UBA)

1.9.1. Implementar respuestas automatizadas a amenazas, como desconectar sesiones de usuarios sospechosos o apagar sistemas infectados.

1.9.2. Detectar anomalías en inicios de sesión mediante aprendizaje automático, como picos en fallos de autenticación o accesos remotos inusuales. CRITERIO CUANTIFICABLE.

1.9.3. Identificar amenazas ocultas observando cambios repentinos en el comportamiento de usuarios, como ejecución de procesos no habituales o múltiples bloqueos de cuenta. CRITERIO CUANTIFICABLE.

1.9.4. Mejorar la inteligencia de amenazas actualizando el comportamiento base de los usuarios continuamente.

1.9.5. Generar informes completos sobre actividades anómalas detectadas en la organización.

1.10. Detección y mitigación de ataques a AD

1.10.1. Panel de control especializado para obtener información clave sobre amenazas en el entorno de AD.

1.10.2. Aplicar reglas basadas en estándares de la industria para identificar indicadores de exposición en AD.

1.10.3. Detectar y remediar indicadores de compromiso estándar del AD.

1.10.4. Detectar y remediar indicadores de compromiso de Kerberos incluyendo Kerberoasting y ataques Golden/Silver Ticket.

1.10.5. Registrar detalles sobre el origen, responsable y método del ataque.

1.10.6. Obtener un historial detallado de las acciones del atacante antes y después del incidente.

1.10.7. Recibir alertas inmediatas sobre intentos en curso de ataques contra AD.

1.10.8. Detectar y prevenir abusos de privilegios mediante la monitorización de acciones de cuentas de alto nivel.

1.10.9. Activar alertas instantáneas ante actividades sospechosas como cambios en el esquema de AD o roles FSMO.

1.10.10. Utilizar análisis de comportamiento para detectar anomalías como picos de bloqueos o inicios de sesión fallidos.

1.10.11. Automatizar respuestas a incidentes como amenazas internas desconectando sesiones sospechosas. CRITERIO CUANTIFICABLE.

1.11. Sistema de alertas en tiempo real

1.11.1. Recibir notificaciones sobre eventos de seguridad en todo el entorno de servidores Windows.

1.11.2. Proporcionar detalles completos sobre cada evento (quién, qué, cuándo y dónde).

1.11.3. Configurar alertas con facilidad y recibirlas por correo electrónico o SMS.

1.11.4. Definir disparadores basados en volumen, tiempo, usuario y otros criterios para reducir alertas innecesarias.

1.11.5. Minimizar falsos positivos con umbrales de alerta dinámicos mediante análisis de comportamiento.

1.11.6. Implementar respuestas automatizadas para reducir el impacto de brechas de seguridad.

Casos de uso de alertas:

1.11.7. Detectar ataques de fuerza bruta: Alertas por múltiples intentos fallidos de inicio de sesión en poco tiempo.

1.11.8. Proteger cuentas críticas: Notificación cuando un usuario se añade a un grupo de seguridad.

1.11.9. Identificar accesos sospechosos: Alertas cuando se accede a un servidor fuera del horario laboral.

1.11.10. Detectar ransomware: Notificación ante un alto volumen de accesos a archivos por un solo usuario. CRITERIO CUANTIFICABLE.

1.12. Monitorización, auditoría e informes del servicio DNS Server.

1.12.1. Auditar y reportar de cambios en configuración del servicio DHCP

1.12.2. Auditar y reportar cambios, altas y bajas en Nodos DNS

1.12.3. Auditar y reportar cambios, altas y bajas de Zonas DNS

1.12.4. Auditar y reportar cambios en permisos DNS

1.13. Monitorización, auditoría de cambios e informes sobre Windows ADCS.

1.13.1. Auditar y reportar el estado de las peticiones de certificado

1.13.2. Auditar y reportar solicitudes de certificado modificadas

1.13.3. Auditar y reportar propiedades de la CA modificadas

1.13.4. Auditar y reportar claves recuperadas recientemente

1.13.5. Auditar y reportar cambios en plantillas de certificados

1.14. Auditoría de Active Directory Federation Services (AD FS)

- 1.14.1. Seguimiento de la actividad de inicio de sesión a través de servidores AD FS.
- 1.14.2. Captura de inicios de sesión exitosos con detalles de IP, aplicación accedida y reclamaciones emitidas.
- 1.14.3. Identificación de intentos fallidos de inicio de sesión, posibles ataques de fuerza bruta y bloqueos extranet.
- 1.14.4. Alertas de eventos clave de AD FS, incluyendo inicios de sesión fuera del horario laboral.

1.15. Replicación e integridad del AD

- 1.15.1. Supervisión del estado de replicación, tráfico de replicación y fallos de replicación. CRITERIO CUANTIFICABLE.
- 1.15.2. Información detallada sobre cambios en equipos del AD (creación, modificación, eliminación, habilitación, deshabilitación y cambios de atributos). CRITERIO CUANTIFICABLE.

2. Requisitos de auditoría y gestión sobre Azure EntraID / Azure Active Directory

2.1. Auditoría de Azure AD

- 2.1.1. Supervisar los inicios de sesión y eventos en Azure Active Directory en entornos en la nube o híbridos.
- 2.1.2. Mantener control detallado de todas las actividades en entornos AD locales, en la nube o híbridos desde una única consola.
- 2.1.3. Conservar registros precisos de la actividad de inicio de sesión de los usuarios de Azure AD, identificando intentos exitosos, fallidos y sospechosos.
- 2.1.4. Examinar cambios realizados en usuarios, grupos, dispositivos, aplicaciones, roles, licencias y directorios en Azure AD.
- 2.1.5. Crear alertas personalizadas para recibir notificaciones inmediatas sobre eventos críticos, como por ejemplo asignación del rol de Administrador Global a un usuario invitado.

2.1.6. Correlacionar el AD híbrido con información contextual como SID, GUID y DN de los usuarios en el entorno local.

2.1.7. Informes preconfigurados de cumplimiento con normativas SOX, HIPAA, FISMA, GLBA, GDPR e ISO.

2.2. Supervisión de inicios de sesión en Azure AD

2.2.1. Monitorizar todos los inicios de sesión en Azure AD y generar informes sobre la actividad de los usuarios.

2.2.2. Generar informes de intentos fallidos de inicio de sesión y causa del fallo.

2.2.3. Analizar patrones de inicio de sesión y detectar eventos sospechosos.

2.2.4. Rastrear los inicios de sesión según el método de MFA utilizado, identificando fallos y obteniendo información sobre su uso. **CRITERIO CUANTIFICABLE.**

2.2.5. Identificar usuarios que intentan iniciar sesión con contraseñas expiradas, antiguas o débiles recientemente creadas.

2.2.6. Detectar bloqueos de cuentas en Azure AD y posibles ataques de fuerza bruta.

2.3. Seguimiento de cambios en objetos de usuario

2.3.1. Supervisar las actividades de gestión de usuarios en Azure AD con informes detallados sobre cuentas creadas, eliminadas y actualizadas.

2.3.2. Obtener información sobre quién realizó los cambios, a quién, cuándo y desde dónde, con valores antiguos y nuevos.

2.3.3. Controlar cambios y restablecimientos de contraseñas realizados por usuarios y administradores.

2.3.4. Vigilar las actividades de los administradores de Azure AD e identificar cambios no autorizados.

2.3.5. Informes específicos de cuentas de usuario habilitadas, deshabilitadas o restauradas.

2.3.6. Identificar si un usuario fue creado en el AD local o en la nube mediante el evento de creación del usuario. **CRITERIO CUANTIFICABLE.**

2.4. Gestión de grupos y roles en Azure AD

2.4.1. Informes específicos de creación, eliminación y actualización de grupos en Azure AD.

2.4.2. Detectar la adición o eliminación de un propietario de un grupo, evitando modificaciones no deseadas en su configuración y membresía.

- 2.4.3. Mantener registro de todos los cambios en la membresía de los grupos, incluyendo la adición o eliminación de usuarios externos.
- 2.4.4. Monitorizar los cambios en las licencias asignadas a grupos en Azure AD.
CRITERIO CUANTIFICABLE.
- 2.4.5. Enviar notificaciones inmediatas cuando se actualizan las reglas de membresía dinámica para evitar escalados de privilegios.
- 2.4.6. Supervisar los cambios de roles, rastreando miembros añadidos o eliminados de los roles de Azure AD.

2.5. Gestión de aplicaciones y dispositivos

- 2.5.1. Informes de dispositivos y aplicaciones añadidos, eliminados o actualizados, con detalles sobre quién realizó el cambio y cuándo.
- 2.5.2. Informes detallados sobre usuarios o propietarios añadidos o eliminados de dispositivos registrados en Azure AD.
- 2.5.3. Informes de dispositivos recientemente habilitados o deshabilitados y configuraciones actualizadas.
- 2.5.4. Informes de aplicaciones a las que se ha concedido o revocado acceso.
- 2.5.5. Registrar métricas de uso de aplicaciones y servicios.
- 2.5.6. Supervisar permisos OAuth recientemente añadidos o eliminados para cumplir con los estándares de seguridad en Azure.

2.6. Detección de riesgos en inicios de sesión de Azure

- 2.6.1. Identificar actividades de inicio de sesión de alto riesgo en Azure AD con información detallada sobre el nivel de riesgo, estado y tipo de evento.
- 2.6.2. Marcar intentos de acceso desde direcciones IP anónimas, maliciosas, sospechosas o infectadas con malware.
- 2.6.3. Detectar intentos de inicio de sesión desde cuentas bloqueadas por políticas de acceso condicional.
- 2.6.4. Identificar intentos de inicio de sesión desde credenciales utilizadas simultáneamente en ataques de fuerza bruta.
- 2.6.5. Aislar accesos desde ubicaciones atípicas, características de inicio de sesión desconocidas o credenciales filtradas. **CRITERIO CUANTIFICABLE.**

3. Requisitos de Auditoría y Gestión de Servidores Windows

3.1. Seguimiento de la Actividad de Inicio de Sesión Local

- 3.1.1. Monitorización de intentos de inicio y cierre de sesión en cada servidor local.
- 3.1.2. Detección de comportamientos sospechosos, como inicios de sesión en múltiples computadoras o fuera del horario laboral.
- 3.1.3. Registro detallado de cambios locales de contraseña, reinicios, bloqueos de cuentas e intentos fallidos de inicio de sesión.
- 3.1.4. Resumen rápido de intentos de inicio de sesión exitosos y fallidos, duración de sesión y usuarios con más intentos fallidos.
- 3.1.5. Auditoría de actividad en servicios de terminal mediante RADIUS y Remote Desktop Gateway. CRITERIO CUANTIFICABLE.
- 3.1.6. Registro del historial de inicios de sesión locales y remotos.

3.2. Monitorización de Integridad de Archivos (FIM - File Integrity Monitoring)

- 3.2.1. Supervisión de la integridad de archivos críticos del sistema, registros y programas.
- 3.2.2. Control de accesos a archivos importantes, incluidos archivos del SO y bases de datos.
- 3.2.3. Identificación de eventos críticos como modificaciones no autorizadas o eliminación de archivos de configuración.
- 3.2.4. Alertas en tiempo real sobre cambios sospechosos en archivos, especialmente fuera del horario laboral.

3.3. Auditoría de Dispositivos Extraíbles

- 3.3.1. Monitorización del uso de dispositivos de almacenamiento externo (USB, discos duros, móviles, CD/DVD).
- 3.3.2. Registro detallado de accesos y modificaciones de archivos en dispositivos extraíbles.
- 3.3.3. Detección de conexiones de dispositivos extraíbles a la red. CRITERIO CUANTIFICABLE.
- 3.3.4. Seguimiento de acciones de copiar y pegar archivos desde/hacia dispositivos externos. CRITERIO CUANTIFICABLE.

3.4. Auditoría del Proceso de Creación y Seguimiento de Tareas Programadas

- 3.4.1.Registro de la creación y eliminación de tareas programadas.
- 3.4.2.Monitorización del estado de tareas programadas, incluyendo activación y desactivación.
- 3.4.3.Detección de modificaciones no autorizadas en tareas críticas del sistema.
- 3.4.4.Alertas sobre cambios en tareas programadas.

3.5. Monitorización de Procesos en Windows

- 3.5.1.Seguimiento de la creación y finalización de procesos con detalles sobre el usuario y equipo involucrado.
- 3.5.2.Identificación de programas ejecutados por los usuarios y detección de actividades sospechosas.
- 3.5.3.Alertas en tiempo real sobre procesos anómalos que pueden indicar infección por malware. CRITERIO CUANTIFICABLE.

3.6. Auditoría de Seguridad en Windows Server

- 3.6.1.Detección de cambios en la fecha y hora del sistema para evitar manipulación de registros.
- 3.6.2.Supervisión de eventos críticos como inicios y apagados del sistema.
- 3.6.3.Registro detallado de eventos de seguridad, incluyendo actividad de inicio de sesión, gestión de cuentas y acceso a archivos.
- 3.6.4.Detección de borrado de registros de seguridad.

3.7. Auditoría de Derechos de Usuario y Políticas Locales en Windows Server

- 3.7.1.Monitorización de cambios en permisos críticos como modificación de zona horaria, acceso remoto y gestión de auditorías.
- 3.7.2.Registro de concesión o revocación de permisos de inicio de sesión (acceso remoto, inicio de sesión como servicio, etc.).
- 3.7.3.Auditoría de cambios en políticas locales, incluyendo habilitación o deshabilitación de permisos especiales.
- 3.7.4.Seguimiento de cambios en políticas de seguridad aplicadas mediante Directivas de Grupo o comandos de administración.

3.8. Generación de Informes y Alertas en Tiempo Real

- 3.8.1.Informes personalizables para facilitar la investigación de eventos.

3.8.2. Alertas instantáneas por correo electrónico o SMS ante eventos críticos.

3.8.3. Informes detallados sobre duración de inicio de sesión, intentos fallidos, actividad de procesos y cambios en el sistema.

4. Requisitos Auditoría de sistemas de ficheros (Servidores de ficheros Windows, cabinas NetApp, Nutanix Files y Azure File Shares)

4.1. Monitorización de accesos y cambios en archivos y carpetas

4.1.1. Auditar accesos a archivos y carpetas de sistema en sistemas de archivos locales en servidores Windows.

4.1.2. Auditar accesos exitosos y fallidos en archivos compartidos: creación, lectura, modificación, eliminación, movimiento, cambios de permisos, copia y pegado.

4.1.3. Auditar accesos a archivos y carpetas en sistemas de ficheros alojados en servidores de archivos Windows.

4.1.4. Auditar accesos a archivos y carpetas alojados en cabina NAS NetApp.

4.1.5. Auditar accesos a archivos y carpetas alojados en sistemas de ficheros Nutanix Files. CRITERIO CUANTIFICABLE.

4.1.6. Auditar accesos a archivos y carpetas alojados en sistemas de ficheros Azure File Shares.

4.1.7. Supervisar cambios en archivos y carpetas en sistemas de ficheros alojados en servidores de archivos Windows.

4.1.8. Supervisar cambios en archivos y carpetas en sistemas de ficheros alojados en cabinas NAS NetApp.

4.1.9. Supervisar cambios en archivos y carpetas en sistemas de ficheros alojados en sistemas de ficheros Nutanix Files. CRITERIO CUANTIFICABLE.

4.1.10. Supervisar cambios en archivos y carpetas en sistemas de ficheros alojados en sistemas de ficheros Azure File Shares.

4.1.11. Auditar cambios en archivos, incluyendo intentos fallidos de modificación, quién cambió qué archivo o carpeta, cuándo y desde dónde.

4.1.12. Controlar derechos de acceso a los datos.

4.1.13. Registrar cambios de permisos y comparar valores anteriores y actuales de ACL.

4.1.14. Registrar cambios de propietario, con detalles de los valores antes y después del cambio.

4.2. Detección de anomalías y alertas de seguridad

- 4.2.1. Identificar actividades inusuales en archivos mediante aprendizaje automático.
- 4.2.2. Detectar cambios no autorizados y envío de alertas inmediatas por correo electrónico y SMS.
- 4.2.3. Definir umbrales para detectar eventos masivos de cambios en archivos.
CRITERIO CUANTIFICABLE.
- 4.2.4. Ejecutar scripts automáticos para responder a amenazas, como apagar dispositivos cuando se active una alerta. **CRITERIO CUANTIFICABLE.**
- 4.2.5. Generar alertas instantáneas y utilizar análisis de comportamiento del usuario (UBA) para detectar anomalías de acceso.
- 4.2.6. Informes preconfigurados de cumplimiento con regulaciones como SOX, HIPAA, PCI DSS, GDPR, FISMA y GLBA.

5. Requisitos de Gestión de Accesos Privilegiados (PAM)

5.1 Gestión de elevación y delegación de privilegios

- 5.1.1 Asignación de controles Just-in-Time para cuentas de dominio y otorgar privilegios elevados solo cuando sea necesario.
- 5.1.2 Revocación automática de permisos de las cuentas después de un período determinado.
- 5.1.3 Restablecimiento automático de contraseñas tras el periodo de uso.

5.2 Controles de confianza cero (Zero Trust)

- 5.2.1 Controles Zero Trust listos para usar.
- 5.2.2 Mecanismo integral de puntuación de confianza para usuarios y dispositivos.
- 5.2.3 Controles de acceso basados en políticas (PBAC).

5.3 Monitorización de sesiones privilegiadas:

- 5.3.1 Supervisión de la actividad de los usuarios privilegiados.
- 5.3.2 Capturar sesiones y archivarlas como archivos de video. **CRITERIO CUANTIFICABLE.**
- 5.3.3 Supervisión de actividad con sesión shadowing.
- 5.3.4 Control dual sobre accesos privilegiados.
- 5.3.5 Supervisar y regular cada actividad de acceso privilegiado en la empresa desde una consola unificada.

5.4 Gestión de privilegios de endpoint:

- 5.4.1 Gestión de privilegios de endpoint de extremo a extremo.
- 5.4.2 Revocación de cuentas de administrador local innecesarias.

- 5.4.3 Acceso Just-in-Time a aplicaciones y procesos específicos, permitiendo o bloqueando su ejecución.

5.5 Análisis del comportamiento de usuarios privilegiados

- 5.5.1 Detección de anomalías por IA y ML para identificar actividades privilegiadas inusuales.
- 5.5.2 Consolidación de datos de acceso privilegiado con registros de eventos de endpoints. CRITERIO CUANTIFICABLE.
- 5.5.3 Captura de todos los eventos relacionados con las operaciones de cuentas privilegiadas.
- 5.5.4 Informes personalizables sobre datos de acceso y actividad de usuarios.

5.6 Integración con aplicaciones y automatización

- 5.6.1 Existencia de SDK, APIs globales y conectores para integrar las acciones de PAM en las aplicaciones.
- 5.6.2 Integración de seguridad de contraseñas en los pipelines de DevOps.
- 5.6.3 Protección de las plataformas de integración y entrega continua contra ataques basados en credenciales.
- 5.6.4 APIs seguras que permitan la integración de aplicaciones eliminando la necesidad de codificación de credenciales.
- 5.6.5 Integración de las rutinas de acceso privilegiado en los flujos de trabajo empresariales mediante la integración de los fundamentos de PAM con aplicaciones empresariales comunes.
- 5.6.6 Integración con sistemas de ticketing para la aprobación de acceso para cuentas privilegiadas y autorizar la recuperación de credenciales.

5.7 Bóveda de credenciales empresarial

- 5.7.1 Escaneado de redes y descubrimiento de activos y cuentas críticas. CRITERIO CUANTIFICABLE.
- 5.7.2 Incorporación automática de las cuentas privilegiadas en una bóveda segura que ofrezca gestión centralizada, cifrado AES-256 y permisos de acceso basados en roles. CRITERIO CUANTIFICABLE.
- 5.7.3 Protección y custodia de certificados SSL e identidades digitales, integrándose con autoridades de certificación estándar. CRITERIO CUANTIFICABLE.

5.8 Acceso remoto seguro RDP, SSH y control remoto

- 5.8.1 Permitir a los usuarios privilegiados lanzar conexiones directas a hosts remotos sin necesidad de agentes en el endpoint, complementos de navegador o programas auxiliares, canalizadas a través de pasarelas encriptadas.
- 5.8.2 Descubrimiento de dispositivos SSH en la red y recopilación de sus claves.
- 5.8.3 Creación y despliegue de nuevos pares de claves SSH.
- 5.8.4 Cumplimiento estricto de políticas para la rotación periódica automatizada de claves.

6 Requisitos de Gestión de Parches y Actualizaciones Windows

6.1 Automatización del Proceso de Parcheado

- 6.1.1 Escaneo y detección automática de parches faltantes.

- 6.1.2 Descarga automática de parches desde sitios de proveedores.
- 6.1.3 Pruebas previas a la implementación para evitar fallos.
- 6.1.4 Implementación automatizada de parches en los sistemas requeridos.
- 6.1.5 Soporte para la actualización automática de definiciones de antivirus de Microsoft Defender. **CRITERIO CUANTIFICABLE.**

6.2 Priorización Basada en la Severidad

- 6.2.1 Clasificación de parches según su criticidad (Crítico, Alto, Moderado, Bajo).
- 6.2.2 Implementación prioritaria de parches críticos y de alta severidad.
- 6.2.3 Programación de parches de menor severidad según ciclos regulares.

6.3 Pruebas Antes de la Implementación

- 6.3.1 Creación de grupos de prueba para evaluar la estabilidad de los parches.
- 6.3.2 Implementación controlada antes de desplegar parches a toda la red.
- 6.3.3 Opción de aprobar automáticamente los parches exitosos tras la fase de prueba.

6.4 Ventanas de Implementación Flexibles

- 6.4.1 Posibilidad de programar despliegues en múltiples días o semanas.
- 6.4.2 Equilibrio entre seguridad de la red y productividad de los empleados.

6.5 Reintento de Implementación de Parches Fallidos

- 6.5.1 Generación de reportes de estado para identificar parches fallidos.
- 6.5.2 Reimplementación automática de parches no instalados debido a errores de red o inactividad del sistema.

6.6 Generación de Informes y Cumplimiento

- 6.6.1 Creación de informes detallados sobre el estado de los parches.
- 6.6.2 Visibilidad total del proceso para auditorías y cumplimiento normativo.
- 6.6.3 Monitorización del estado de salud de los sistemas según la cantidad de parches faltantes.

6.7 Compatibilidad con las versiones de Windows Server Standard, Enterprise y Datacenter siguientes:

- 6.7.1 Windows Server 2012
- 6.7.2 Windows Server 2012 R2
- 6.7.3 Windows Server 2016
- 6.7.4 Windows Server 2019
- 6.7.5 Windows Server 2022
- 6.7.6 Windows Server 2025

6.8 Gestión de Diferentes Tipos de Actualizaciones

- 6.8.1 Actualizaciones de seguridad (Críticas a Baja severidad).
- 6.8.2 Paquetes de servicio y paquetes de características.
- 6.8.3 Rollups y actualizaciones opcionales.
- 6.8.4 Actualizaciones no relacionadas con seguridad.

6.9 Actualizaciones de servidores Windows fuera de dominio

- 6.9.1 Automatización del proceso de parcheo en servidores Windows fuera de dominio (por ejemplo, en DMZ) en las mismas condiciones que los servidores en dominio: detección de parches faltantes, descarga automática, prueba e instalación de parches desatendida.
- 6.9.2 Aplicación de configuraciones estándar de forma remota centralizada a un grupo de servidores fuera de dominio.
- 6.9.3 Gestión de usuarios locales y contraseñas de manera centralizada a un grupo de servidores fuera de dominio.
- 6.9.4 Modificación de claves de registro de manera centralizada a un grupo de servidores fuera de dominio.
- 6.9.5 Ejecución remota de scripts de lenguajes estándar (cmd, powershell, Python VBScript, JScript,...) en un grupo de servidores fuera de dominio.

6.10 Despliegue de parches de Aplicaciones de Terceros

- 6.10.1 Capacidad para desplegar parches de aplicaciones de terceros
- 6.10.2 Despliegue de parches de Oracle Java y OpenJDK
- 6.10.3 Despliegue de parches de Google Chrome
- 6.10.4 Despliegue de parches de Adobe Acrobat
- 6.10.5 Despliegue de parches de Horizon View. CRITERIO CUANTIFICABLE.
- 6.10.6 Despliegue de parches de Git. CRITERIO CUANTIFICABLE.

6.11 Administración Centralizada y Control Total

- 6.11.1 Consola centralizada para gestionar la implementación de parches.
- 6.11.2 Compatibilidad con redes basadas en Active Directory y grupos de trabajo.
- 6.11.3 Programación y automatización de todo el ciclo de gestión de parches.

6.12 Gestión de Parches Sensibles

- 6.12.1 Posibilidad de excluir ciertos parches que puedan generar incompatibilidades.
- 6.12.2 Bloqueo selectivo de actualizaciones en grupos de dispositivos o aplicaciones específicas.

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

RNF1- El software propuesto debe ser gestionable desde una única consola, o en su defecto formar parte de la misma suite de productos del mismo fabricante para trabajar de manera integrada.

RNF2- El software propuesto debe instalarse en modalidad on-prem.

RNF3 - El software propuesto no puede transmitir ni almacenar ningún tipo de información personal en cloud público o privado.

RNF4 - El licenciamiento del producto debe cumplir con las necesidades del entorno Windows de Canal, consistente en:

- 500 servidores Windows
- 1 dominio con 5 domain controllers
- 1 tenant Azure
- 50 técnicos administradores

I.3. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

Vigencia de las licencias:

Programa	Periodo de vigencia del licenciamiento
Software de auditoría y administración de servidores Windows	36 meses

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

Programa	Derechos durante la vigencia de las licencias
Licenciamiento por servidor/equipo	• Derecho de uso: por servidor o equipo. 500 servidores • Derecho de actualización: parches de seguridad, versiones menores, versiones mayores • Derecho de acceso a documentación • Derecho de consulta al fabricante (soporte del fabricante): ○ Horario: Lunes a viernes 8:00 a 17:00 • Tiempo de respuesta: 5 días laborables • Otros derechos:
Licenciamiento por controlador de dominio	• Derecho de uso: por dominio o controlador de dominio. 1 dominio, 5 DCs • Derecho de actualización: parches de seguridad, versiones menores, versiones mayores • Derecho de acceso a documentación • Derecho de consulta al fabricante (soporte del fabricante): ○ Horario: Lunes a viernes 8:00 a 17:00 ○ Tiempo de respuesta: 5 días laborables • Otros derechos
Licenciamiento por técnico administrador	• Derecho de uso: por usuario administrador. 50 técnicos administradores • Derecho de actualización: parches de seguridad, versiones menores, versiones mayores • Derecho de acceso a documentación:

	• Derecho de consulta al fabricante (soporte del fabricante): ○ Horario: Lunes a viernes 8:00 a 17:00 ○ Tiempo de respuesta: 5 días laborables • Otros derechos
--	--

El software puede ser ofertado en modo licencia perpetua (con soporte de fabricante y actualizaciones durante los 36 meses de duración del contrato) o en modo suscripción. Canal de Isabel II, S.A., M.P. prefiere el modo licencia perpetua y esta opción es valorada en los criterios evaluables.

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

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

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

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

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

II.1. SERVICIOS DE INSTALACIÓN AVANZADA DE LOS PROGRAMAS A SUMINISTRAR

Alcance

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

El alcance del servicio de instalación avanzada incluye el estudio del entorno, la instalación de los productos, las configuraciones de los productos, las cargas de datos e integraciones con el resto del entorno necesarias para la explotación de los mismos.

Estas actuaciones deben realizarse de forma conjunta con los servicios de administración de sistemas de Canal de Isabel II, S.A., M.P. y deben realizarse sin pérdida de servicio.

Hitos y entregables

Hito	Descripción del hito y sus entregables	Plazo	Porcentaje de la prestación
HITO_01	Estudio del entorno y preparación de la implantación. Entregables: Plan de implantación	15 días a partir del inicio de la ejecución	0%
HITO_02	Instalación, configuración y puesta en marcha de la auditoría/administración del directorio activo. Entregables: - Producto instalado y configurado - Documentación técnica de la instalación y configuración - Documentación técnica de los procedimientos de operación	1 mes después de la aceptación del HITO_01	15%
HITO_03	Instalación, configuración y puesta en marcha de la auditoría/administración del Azure EntraID. Entregables: - Producto instalado y configurado - Documentación técnica de la instalación y configuración - Documentación técnica de los procedimientos de operación	1 mes después de la aceptación del HITO_01	15%
HITO_04	Instalación, configuración y puesta en marcha de la auditoría/administración de los servidores Windows. Entregables: - Producto instalado y configurado - Documentación técnica de la instalación y configuración - Documentación técnica de los procedimientos de operación	1 mes después de la aceptación del HITO_01	15%
HITO_05	Instalación, configuración y puesta en marcha de la auditoría de los sistemas de ficheros. Entregables:	1 mes después de la aceptación	15%

	• Producto instalado y configurado • Documentación técnica de la instalación y configuración • Documentación técnica de los procedimientos de operación	del HITO_01	
HITO_06	Instalación, configuración y puesta en marcha de la gestión de accesos privilegiados. Entregables: • Producto instalado y configurado • Documentación técnica de la instalación y configuración • Documentación técnica de los procedimientos de operación	1 mes después de la aceptación del HITO_01	25%
HITO_07	Instalación, configuración y puesta en marcha de la gestión de parches y actualizaciones. Entregables: • Producto instalado y configurado • Documentación técnica de la instalación y configuración • Documentación técnica de los procedimientos de operación	En caso de que Canal lo requiera, 1 mes después de la solicitud de Canal de Isabel II, S.A., M.P.)	15%

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

Alcance

Las tareas incluidas en el soporte a prestar por el adjudicatario son las siguientes:

- Resolución de dudas funcionales de las herramientas suministradas
- Soporte técnico de nivel 1 y 2, capaz de identificar y resolver los problemas o defectos conocidos en la documentación del fabricante o que respondan a errores de configuración del mismo.
- Escalado y seguimiento de incidencias de producto a fabricante (nivel 3 de soporte).
- Suministro de parches y actualizaciones de versiones del software.
- Soporte a la actualización de versiones de los productos.
- Soporte a la integración de los productos ofertados con otros sistemas corporativos.

Horario de servicio

El horario de servicio será de lunes a viernes de 8:00 a 17:00 horas.

II.2.1. DIMENSIONAMIENTO DEL SERVICIO

El dimensionamiento previsto es el equivalente a 5 jornadas anuales.

II.2.2. ACUERDOS DE NIVEL DE SERVICIO

A efectos de cálculo del cumplimiento de los ANS, sólo computa el tiempo transcurrido dentro del horario de prestación del servicio descrito en el apartado anterior y atendiendo al dimensionamiento anterior. No se considerará el incorrecto desempeño del contratista por incumplimiento de los ANS si las incidencias superan el dimensionamiento del servicio previstos en el apartado anterior.

Id.	Nombre	Descripción del indicador	Valor
ANS_01	Tiempo de respuesta	Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de soporte comunica que ha empezado a trabajar en su resolución.	4 horas
ANS_02	Tiempo de resolución de incidencia leve	Tiempo transcurrido desde el final del tiempo de respuesta hasta que el equipo de soporte ha solucionado la incidencia. No incluye el tiempo necesario para la aprobación por el Responsable del Contrato Específico. Incidencia leve: Sin afección a los servicios productivos. Incidencia grave: Afección a servicios productivos que no impida el acceso a los servicios. Incidencia crítica: Imposibilidad de acceso a servicios de producción.	72 horas
ANS_03	Tiempo de resolución de incidencia grave		24 horas
ANS_04	Tiempo de resolución de incidencia crítica		8 horas
ANS_05	Tiempo de resolución de soporte	Tiempo transcurrido desde que se comunica una necesidad de soporte no relacionada con una incidencia hasta que se responde la solicitud de soporte	5 días laborables

Cuando la resolución de la incidencia requiera la realización de desarrollos que por su naturaleza necesitan de un plazo material superior al indicado en la tabla precedente, el contratista estará obligado a presentar al Responsable del Contrato Específico en el organismo destinatario, dentro del plazo de tiempo de resolución inicial, un plan de actuación que incluya la duración prevista de los trabajos para la resolución, la justificación de dicha previsión y la descripción de los trabajos a realizar. Si es necesario, se incluirá la descripción de las medidas paliativas a adoptar hasta la completa resolución de la incidencia. Dicho plan deberá ser aprobado por el Responsable del Contrato Específico.

II.3. REQUISITOS DE LOS PERFILES PROFESIONALES

La persona o personas que provean los servicios de instalación avanzada descritos en el apartado II.1 de este anexo deben contar con certificación oficial del fabricante en las soluciones ofertadas.

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

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

Si en el apartado IV.2.1 se ha indicado que existe tratamiento de datos personales, a continuación, se señalan los datos personales que se van a transmitir y almacenar en la nube objeto del suministro:

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

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

III.2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

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

Los productos solicitados deben instalarse on-prem y no deben transmitir ni almacenar ningún dato personal en la nube, de acuerdo a las especificaciones no funcionales requeridas en este documento.

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato y/o información que pudiera conocer o le fuese facilitado con ocasión de la ejecución del contrato y vendrá obligado a garantizar y comprometerse de manera expresa a respetar el deber de secreto y confidencialidad y actuar acorde a la normativa de secreto empresarial, respecto a los datos e informaciones que hubiera podido conocer con motivo de la ejecución del contrato, especialmente los de carácter personal o empresarial, información confidencial y/o que constituya secreto empresarial, que no podrá copiar o utilizar con fin distinto, ni tampoco ceder a otros ni siquiera a efectos de conservación. En todo caso, el contratista actuará en el tratamiento de los datos únicamente de conformidad con las instrucciones que le señale Canal de Isabel II, S.A., M.P. La obligación de preservar la confidencialidad rige durante el desarrollo del Contrato y con posterioridad al mismo. A tal efecto, el contratista se obliga a indemnizar a Canal de Isabel II, S.A., M.P., por cualesquiera daños y perjuicios que sufra directamente, o por toda reclamación, acción o procedimiento, que traiga su causa de un incumplimiento o cumplimiento defectuoso por parte del contratista de lo

dispuesto tanto en los Pliegos, como en el contrato y como en lo dispuesto en la normativa reguladora de la protección de datos personales.

El contratista devolverá a Canal de Isabel II, S.A., M.P. la información confidencial y todas sus copias, o la destruirá dando prueba de ello. La devolución o destrucción de la información no eximirá al contratista del cumplimiento de confidencialidad aquí reflejado.

El contratista sólo podrá revelar la información confidencial y/o datos personales a sus empleados, con la finalidad de realizar el trabajo objeto del contrato y será responsable de los actos de los mismos.

Canal de Isabel II, S.A., M.P. tendrá derecho a exigir en cualquier momento que la información confidencial proporcionada al contratista, sea destruida o devuelta, ya sea antes, durante o después de la celebración del contrato.

Los datos personales facilitados por el contratista serán incluidos en las actividades de tratamiento de contratación de Canal de Isabel II, S.A., M.P. con la finalidad de gestionar el objeto del presente procedimiento, en base a la aplicación de medidas precontractuales y contractuales y/o como consecuencia de una obligación legal, así como el interés legítimo de Canal de Isabel II, S.A., M.P. de relacionarse dentro del ámbito del presente procedimiento. Los datos serán tratados mientras dure el procedimiento y una vez hayan finalizado las responsabilidades nacidas durante el tratamiento de datos y/o el procedimiento. El ejercicio de los derechos de acceso, rectificación, supresión y/o demás derechos reconocidos en la normativa de protección de datos, podrán ser ejercidos en el domicilio social de Canal de Isabel II, S.A., M.P. en Calle Santa Engracia, 125, 28003, Madrid o remitiendo un correo a privacidad@canal.madrid.

Canal de Isabel II, S.A., M.P., en cumplimiento de lo dispuesto en la normativa relativa a transparencia podrá publicar, en el apartado de Transparencia de su página web y/o en los sitios web que proceda, parte del contenido del presente procedimiento, lo que podría provocar la publicación de ciertos datos personales identificativos, o bien, el acceso a los mismos, por parte de los solicitantes que pudieran estar legitimados para acceder a la información pública. Asimismo, podrá ser necesario como consecuencia de una obligación legal facilitar en determinados supuestos información a Juzgados y Tribunales, Agencia Tributaria, Cámara de Cuentas, etc.

En cuanto a los datos personales que los licitadores faciliten en la fase de licitación al objeto de comprobar la adscripción de medios personales, los criterios de solvencia y los criterios de valoración de la oferta, si procede, serán tratados por Canal de Isabel II, S.A., M.P. en base a la aplicación de medidas precontractuales y por obligación legal. Los datos serán tratados mientras dure el procedimiento y una vez hayan finalizado las obligaciones legales aplicables.

Canal de Isabel II, S.A., M.P. podrá tratar los datos personales de los empleados del contratista o del personal subcontratado -en caso de que aplique subcontratación y haya sido autorizado para ello-, comunicados por el contratista en la fase de ejecución del contrato, en base al interés legítimo de Canal de Isabel II, S.A., M.P. de relacionarse dentro del ámbito del presente pliego, así como al objeto de realizar la comprobación de los medios humanos comprometidos y adscritos a la ejecución del contrato, y en su caso, para cumplir la normativa de prevención de riesgos laborales y de coordinación de actividades empresariales, de derechos de las personas con discapacidad y de su inclusión social. Del mismo modo, los datos personales de los empleados del contratista podrán ser tratados con la finalidad de resolver las notificaciones relativas al Código Ético y de Conducta, y la Política de Cumplimiento de Canal de Isabel II, S.A., M.P., ya sea como consecuencia de comunicaciones que el empleado realice por su propia iniciativa o como consecuencia de comunicaciones realizadas por terceras personas, y para gestionar las correspondientes autorizaciones de acceso a las instalaciones de Canal de Isabel II, S.A., M.P. que puedan ser necesarias por motivos de seguridad. En este sentido, para garantizar la seguridad, emitir tarjetas y/o llaves mecánicas para la realización de controles de acceso a las instalaciones y/o para valorar la correcta ejecución del contrato, Canal de Isabel II, S.A., M.P. podría necesitar información del personal adscrito a la ejecución del mismo, en concreto requerirá nombre y apellidos, DNI, fecha de expedición y vigencia del contrato, etc. y/o la captación de la imagen de dicho personal y/o la aportación de fotografías con el formato que indique Canal de Isabel II, S.A., M.P., a elección de esta. Los datos serán tratados mientras dure el Contrato y una vez hayan finalizado las obligaciones legales aplicables.

En cualquier caso, será responsabilidad de los licitadores contar con los consentimientos necesarios y facilitar toda la información que corresponda a las personas físicas en relación con el tratamiento de los datos personales que vayan a facilitar a Canal de Isabel II, S.A., M.P., con las finalidades y legitimaciones indicadas en párrafos precedentes. Asimismo, deberán informar expresamente a esas personas físicas de que pueden acceder, rectificar, oponerse o suprimir sus datos y demás derechos reconocidos en la normativa de protección de datos, en la dirección social de Canal de Isabel II, S.A., M.P. con la referencia RGPD o bien por correo electrónico en la dirección privacidad@canal.madrid. No será imputable a Canal de Isabel II, S.A., M.P. la omisión de este deber de información por parte de los licitadores respecto a las personas físicas que adscriban a la ejecución del contrato.

ANEXO IV NECESIDAD DE PRODUCTOS CONCRETOS POR COMPATIBILIDAD CON INSTALACIÓN EXISTENTE

Contratos previos asociados con la instalación existente:

Contrato	Fecha adjudicación	Importe	Objeto
Enlace al contrato 1 en el perfil del contratante	Fecha de adjudicación	Importe de adjudicación	Breve descripción del objeto del contrato
Enlace al contrato 2 en el perfil del contratante	Fecha de adjudicación	Importe de adjudicación	Breve descripción del objeto del contrato
...	...	...	...

Justificación de la instalación existente y de la necesidad de compatibilidad con la misma, que haría técnicamente inviable el uso de otras soluciones, o justificación de costes desproporcionados en caso de cambio.

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

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

D./D^a....., con D.N.I. n^o....., actuando en nombre propio / en representación de (a empresa licitadora) con N.I.F.:....., con domicilio (de la empresa licitadora) en (calle/plaza/etc.):....., n^o....., Población:....., Provincia:....., y código postal:.....

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

DECLARA

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

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

Detalle de las medidas de seguridad aplicables	
--	--

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

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

(Fecha, firma y nombre completo del representante legal)

Fdo. electrónicamente

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

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

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

MANIFIESTO

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

Indicar nombre y cargo. Firma electrónica.

ANEXO VII ENTREGAS PARCIALES

<i>Entrega 1: descripción de las licencias a entregar</i>	<i>Número máximo de días naturales desde la notificación de la adjudicación</i>	<i>Datos del lugar de entrega</i>
<i>Entrega 2: descripción de las licencias a entregar</i>	<i>Número máximo de días naturales (contados desde algún hito concreto)</i>	<i>Datos del lugar de entrega</i>
<i>Entrega 3: descripción de las licencias a entregar</i>	<i>Número máximo de días naturales (contados desde algún hito concreto)</i>	<i>Datos del lugar de entrega</i>
...	...	...

ANEXO VIII COBERTURA DE LA GARANTÍA EXTENDIDA DEL ADJUDICATARIO

La garantía extendida que debe prestar el adjudicatario durante todo el periodo de vigencia de las licencias se rige por lo descrito en el apartado III.8 del Pliego de Prescripciones Técnicas:

- Soporte de nivel 1 y nivel 2 prestado por el adjudicatario a petición del organismo destinatario, en los términos descritos en el PPT;
- Soporte del adjudicatario al organismo para el acceso a la garantía del fabricante (acceso al soporte de nivel 3), en los términos descritos en el PPT;
- Soporte a la instalación de actualizaciones, en los términos descritos en el PPT;
- Cobertura ante posibles problemas jurídicos derivados de la aplicación de las cláusulas de *términos y condiciones* del fabricante, en los términos descritos en el PPT.

Horario de contacto: Haga clic o pulse aquí para escribir texto.

Acuerdos de nivel de servicio:

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

ANEXO IX MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN

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

(Indicar:

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

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

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

- **Declaración responsable** de los subcontratistas de no hallarse incurso en prohibición de contratar, conforme el art. 71 de la LCSP.¹¹
- **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

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

ANEXO X MODELO DE PROPOSICIÓN ECONÓMICA

CANAL DE ISABEL II, S.A., M.P.

Santa Engracia, 125

D., con D.N.I., en nombre y representación de, con domicilio social en enterado de las condiciones, requisitos y obligaciones establecidos en el documento de licitación referido al **CONTRATO DE SOFTWARE DE AUDITORÍA Y ADMINISTRACIÓN DE SERVIDORES WINDOWS (Exp.: 236/2025)**, cuyo contenido declara conocer y acepta plenamente, se compromete a tomar a su cargo la ejecución del Contrato, en las siguientes condiciones:

<i>artículo (clave catálogo)</i>	<i>Nº unidades requeridas</i>	<i>Descripción</i>	<i>Precio unitario IVA excluido (máximo dos decimales) (€)</i>	<i>Importe TOTAL IVA excluido (máximo dos decimales) (€)</i>
<i>Licencias de software para gestión de infraestructura (Lote 2)</i>	02.01.00.XXX	500	<i>Licencias ofertadas por equipo/servidor</i>	
<i>Licencias de software para gestión de infraestructura (Lote 2)</i>	02.01.00.XXX	5	<i>Licencias ofertadas por controlador de dominio</i>	
<i>Licencias de software para gestión de infraestructura (Lote 2)</i>	02.01.00.XXX	50	<i>Licencias ofertadas por administrador</i>	
<i>Servicios complementarios – Instalación avanzada (Lote 2)</i>	02.02.00.XXX	1	<i>Proyecto de instalación y configuración avanzada</i>	
<i>Servicios complementarios – Soporte del</i>	02.03.00.XXX	3	<i>Soporte anual del software</i>	

adjudicatario (Lote 2)					
Importe total IVA excluido (1) (€)					
Importe IVA (€)					
IMPORTE TOTAL IVA incluido (€)					

(1) El licitador no podrá exceder del importe máximo de licitación establecido en 156.000,00 €, IVA excluido, para la duración del contrato. En caso contrario la oferta del licitador no se tendrá en consideración.

(2) El licitador no podrá exceder en su oferta el presupuesto correspondiente a suministro de licencias indicado en el apartado 4.1 para la suma total de los apartados de suministro de licencias.

(3) El licitador no podrá exceder en su oferta el presupuesto correspondiente a cada uno de los servicios indicado en el apartado 4.1 para cada uno de los servicios complementarios, tal como se indica en dicho apartado.

- Complete únicamente las casillas sombreadas en amarillo.
- Actualice el código de la clave del catálogo correspondiente
- Los importes de los servicios complementarios por los conceptos de soporte e instalación avanzada serán inferiores al 50% del importe del contrato.
- El licenciamiento ofertado debe cubrir un parque de 500 servidores, 5 controladores de dominio y 50 usuarios técnicos administradores. Debe rellenar la línea del modo de licenciamiento ofertado, o en caso de que haya distintos ítems de software con distintos modos de licenciamiento las que correspondan a dichos modos de licenciamiento.
- No se aceptarán las proposiciones económicas que contengan omisiones, errores o tachaduras que impidan conocer claramente lo que Canal de Isabel II, S.A., M.P. estime fundamental para considerar la oferta. Si alguna proposición no guardase concordancia con la documentación examinada y admitida, excediese de la base imponible del presupuesto base de licitación del contrato, o en algunas de las partidas/capítulos limitadas explícitamente en el presente Documento de Licitación, variase sustancialmente el modelo establecido, comportase error manifiesto en el importe de la proposición, o existiese reconocimiento por parte del licitador de que adolece de error o inconsistencia que le hagan inviable, será desechada, sin que sea causa bastante para el rechazo el cambio u omisión de algunas palabras del modelo si ello no altera su sentido.
- Cuando la suma de los importes desglosados y/o precios unitarios incluidos en la proposición económica no se corresponda con la cantidad total resultante establecida en la misma, se considerará siempre que el error reside en la cantidad total resultante y no en los precios unitarios.

- En el caso de que en la proposición económica del licitador se consigne algún precio unitario con el valor 0 ó falte algún precio unitario (bien por omisión, bien porque se haya consignado cualquier signo distinto a un número natural o bien porque se quede en blanco), se considerará **tanto a efectos de valoración de la oferta como de ejecución del contrato, que el precio unitario ofertado para ese concepto es 0**. En este caso, el licitador podrá retirar su oferta, no teniendo dicha retirada la consideración de injustificada a los efectos previstos en el artículo 62 del RGLCAP.
- En el caso de que los precios unitarios o el importe de adjudicación tenga más de dos decimales, dicho importe se truncará al segundo decimal, es decir sin redondeos en base al tercer decimal.

ANEXO XI MODELO DE CUMPLIMIENTO DE REQUISITOS Y CRITERIOS AUTOMÁTICOS EVALUABLES MEDIANTE FÓRMULAS

- Cumplimiento de requisitos obligatorios:

Los licitadores deberán cumplimentar y acreditar el cumplimiento de los requisitos obligatorios referidos en el Anexo I y establecidos en la plantilla del Anexo XII.

Los requisitos obligatorios deben acreditarse de uno de los siguientes modos:

- Captura de pantalla de la herramienta donde se muestre la funcionalidad requerida.
- Enlace al apartado de la web del producto donde se indique el cumplimiento del requisito. En caso de que no haya enlace al apartado concreto del requisito, puede incluirse una captura de pantalla del punto donde se referencia el requisito y el enlace a la página completa.
- Anexado de documentación técnica de producto en formato PDF con indicación de la página y línea donde se acredita el cumplimiento del requisito.

La oferta del licitador que no cumpla o acredite todos los requisitos obligatorios no será tenida en cuenta en el presente procedimiento de licitación.

- Criterios automáticos evaluables mediante fórmulas:

Para obtener la valoración indicada en el apartado 7.3.1 del presente documento de invitación los licitadores deberán cumplimentar y acreditar el cumplimiento de los requisitos considerados como criterios cuantificables referidos en el Anexo I y establecidos en la plantilla del Anexo XII.

Los requisitos considerados como criterios cuantificables deberán acreditarse de uno de los siguientes modos:

- Captura de pantalla de la herramienta donde se muestre la funcionalidad requerida.
- Enlace al apartado de la web del producto donde se indique el cumplimiento del requisito. En caso de que no haya enlace al apartado concreto del requisito, puede incluirse una captura de pantalla del punto donde se referencia el requisito y el enlace a la página completa.
- Anexado de documentación técnica de producto en formato PDF con indicación de la página y línea donde se acredita el cumplimiento del requisito.

En caso de discrepancia entre los valores propuestos por el licitador en el Anexo XII y la documentación que, en su caso, se haya solicitado para acreditar dichos valores, se tendrá en consideración en todo caso los valores que resulten de la documentación acreditativa presentada. En los casos en que se solicite un concreto y específico tipo de documentación para

acreditar la realidad de los valores ofertados no se tendrá en cuenta otro tipo de documentación aportada por el licitador.

**ANEXO XII PLANTILLA DE ACREDITACIÓN DE REQUISITOS OBLIGATORIOS Y DE
CRITERIOS CUANTIFICABLES**

Se facilita a los licitadores invitados Anexo XII de acreditación de requisitos obligatorios y de criterios cuantificables que deberán cumplimentar