SISTEMA DINÁMICO DE ADQUISICIÓN DE SUMINISTRO DE EQUIPOS DE COMUNICACIONES, SERVIDORES Y SISTEMAS DE ALMACENAMIENTO - SDA 24/2022

(Expediente nº 2022/68)

INVITACIÓN A LA LICITACIÓN DEL CONTRATO

Renovación de los cortafuegos externos de CSN, con capacidades de IoT

Lote 1 - Equipos de comunicaciones

En virtud de los 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 ***15 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.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

TÉRMINOS Y CONDICIONES

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

Organismo destinatario

Unidad proponente: Subdirección de Tecnologías de la Información
Centro directivo: Secretaría General
Departamento/organismo: Consejo de Seguridad Nuclear

Responsable del contrato (nombre, apellidos, cargo y dependencia orgánica):
Emi Serrano Serrano (Jefa de Área de Sistemas y Comunicaciones - Subdirección de Tecnologías de la Información del CSN)

Datos de **contacto**:

Dirección Postal: Calle Pedro Justo Dorado Dellmans, 11, 28040 MADRID
Correo electrónico: emi.serrano@csn.es
Teléfono: 913460270

Órgano de Contratación:

Dirección General de Racionalización y Centralización de la Contratación.

2 LOTE, TITULO Y OBJETO DEL CONTRATO ESPECÍFICO

2.1 LOTE, TÍTULO Y OBJETO

Lote objeto de licitación: Lote 1 - Equipos de comunicaciones

Título del contrato: Renovación de los cortafuegos externos de CSN, con capacidades de IoT

Objeto del contrato:

El objeto de este contrato es la renovación de los dos cortafuegos externos de CSN, dispositivos de red con capacidad de segmentación, detección de dispositivos de Internet, monitorización y supervisión de los mismos.

El Consejo de Seguridad Nuclear (en adelante CSN) ***precisa*** renovar sus cortafuegos externos para la adecuada gestión de interfaces de acceso, seguridad de las redes LAN e Internet de alta velocidad, protegiendo todo el tráfico que circula por dichas líneas, incluido el cifrado, con capacidades de gestión y prevención de amenazas. Así mismo, necesita **proteger los dispositivos IoT** (Internet de las Cosas) de amenazas desconocidas, en función de recomendaciones de políticas automáticas.

En resumen, se necesita:

Renovar los actuales dos equipos PA-3020, cuyo EOSH (hardware End-of-Support) finaliza en 2024.

- Instalación de los nuevos equipos con la misma arquitectura y configuración de los actuales, y habilitando capacidades de IoT para protección de dispositivos conectados a red CSN de amenazas desconocidas
- Soporte para mantenimiento de los equipos, licencias y su configuración durante 5 años
- Los requisitos funcionales de los equipos se describen en el Anexo I
- Los requisitos de mantenimiento se describen en el Anexo II

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

2.2 CARACTERÍSTICAS PRINCIPALES DE LAS PRESTACIONES

Con respecto a los suministros objeto del contrato específico:

☒ Se adquieren equipamientos en infraestructura local
☒ Se adquiere software embarcado
☐ Se adquiere software con carácter accesorio al suministro de equipamientos
(únicamente posible para el lote 2 y sólo si se ha marcado la primera opción)

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

☒ Se solicita **garantía extendida del adjudicatario** con la cobertura descrita en el apartado III.8 del PPT y concretada en el **Anexo V** de este documento, cuya duración se extenderá durante todo el periodo de vigencia de las licencias objeto del suministro.

☒ Se solicitan **servicios a realizar por el adjudicatario** del contrato específico, para la instalación avanzada o soporte de los suministros. Estos servicios se describen en el **Anexo II**.

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

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

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

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

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

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

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

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

2.3 TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DEL ADJUDICATARIO

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

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

☐ **SÍ. Cláusula aplicable para "Protección de datos con acceso a datos personales".** El contrato SI requiere tratamiento de datos personales por parte del adjudicatario. La finalidad para la que se ceden los datos es: Haga clic o pulse aquí para escribir texto.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

2.4 CATEGORIZACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

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

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

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

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

Relación de los suministros con la arquitectura de seguridad

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

☒ El suministro incluye equipamientos o programas que **forman parte de la arquitectura de seguridad** del sistema de información resultando de aplicación lo previsto en el **apartado 9.3** del documento de invitación[1]. Los suministros objeto del presente contrato específico, que forman parte de la arquitectura de seguridad del organismo destinatario son los siguientes[2]:

- 2 equipos cortafuegos para reemplazar los 2 PA-3020 actuales
- Licencias para dichos cortafuegos

3 DURACIÓN DEL CONTRATO

3.1 FECHA DE INICIO DE LA EJECUCIÓN

El plazo del contrato específico se iniciará:

☒ Al día siguiente al de adjudicación del contrato.

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

3.2 PLAZO DE ENTREGA DE LOS SUMINISTROS

☒ No admite entregas parciales

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

---

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

3.3 PLAZO DE EJECUCIÓN DEL CONTRATO

☒ El equipamiento no requiere instalación ni configuración básica. **Plazo máximo** de entrega[3]: 30 días naturales contados a partir de la fecha de inicio de ejecución del contrato.

☐ Se requiere la instalación y configuración básica de los bienes, incluido en el precio el suministro, en las condiciones del apartado IV.2 del PPT, en el plazo[4] de 50 días naturales, incluido el plazo de entrega de los bienes.

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

- Plazo de ejecución[5]: **2 meses**

☒ El contrato incluye servicios de soporte personalizados a prestar por el adjudicatario a contar desde el final de la instalación básica, y, en su caso, de la instalación avanzada, descritos en el **Anexo II**, apartado 2, en este caso, el plazo de ejecución total del contrato será de **5 años**.

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

3.4 PRÓRROGA DEL CONTRATO ESPECÍFICO

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

4 VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO DE LICITACIÓN

4.1 PRESUPUESTO DE LICITACIÓN Y APLICACIONES PRESUPUESTARIAS

Presupuesto total sin impuestos (€)	Impuestos indirectos (€)	Presupuesto total con impuestos (€)
497.000,00	104.370,00	601.370,00

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

[4] Por defecto, 50 días naturales. El organismo podrá indicar un plazo superior. Este plazo incluye los 30 días naturales para la entrega de los bienes. El cumplimiento del plazo por parte del adjudicatario será exigible cuando el organismo haya puesto a disposición del adjudicatario un entorno limpio en caso de nueva instalación, en un plazo no superior a 20 días hábiles.

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Detalle del presupuesto de licitación:

	Presupuesto sin impuestos (€)	**Impuestos indirectos (€)**	**Presupuesto con impuestos (€)**
SUMINISTRO			
Suministro de equipamientos y, en su caso, software embarcado (incluye extensión de garantía del adjudicatario, si exigida en 2.2)	444.000,00	93.240,00	537.240,00
Elementos complementarios	22.000,00	4.620,00	26.620,00
SERVICIOS			
Servicio de instalación avanzada, a prestar por el adjudicatario	7.000,00	1.470,00	8.470,00
Servicio de soporte, a prestar por el adjudicatario	24.000,00	5.040,00	29.040,00
TOTAL	**497.000,00**	**104.370,00**	**601.370,00**

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

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

Las obligaciones económicas que se deriven para la Administración por el cumplimiento del contrato serán financiadas por el Presupuesto de Gastos del organismo CONSEJO DE SEGURIDAD NUCLEAR, Centro de Gestión 23.302 (MITERD-CSN), con cargo a las siguientes anualidades y aplicaciones presupuestarias:

Aplicación presupuestaria	**Anualidad 2024**	**Anualidad 2025**	**Anualidad 2026**	**Anualidad 2027**	**Anualidad 2028**	**TOTAL**
630.04	578.138,00	5.808,00	5.808,00	5.808,00	5.808,00	**601.370,00**

Conforme a lo establecido en el artículo 103 de la LCSP, **no procederá la revisión de precios** durante la vigencia del contrato.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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	31.000,00 €
Resto costes directos	374.000,00 €
Costes indirectos + Gastos generales + Beneficio industrial	92.000,00 €
Total sin IVA	497.000,00 €

Justificación:

- Suministro:

  Se han estimado los costes en base a precios de los fabricantes para instituciones gubernamentales.
- Trabajos complementarios de instalación avanzados:

  Considerando otros proyectos de similar complejidad técnica y plazo de implantación, se han estimado en base a un consultor y un técnico de sistemas de nivel alto con certificaciones del fabricante, trabajando 200 horas en total a 35 € la hora aproximadamente.
- Soporte:

  Se ha estimado en unas 175 horas anuales por un técnico de sistemas de nivel medio con certificaciones del fabricante, a 35,4 € la hora aproximadamente.
- Costes indirectos:

  Se consideran como tales los costes variables de infraestructura y gastos generales de los posibles licitadores, correspondientes a un 13,41% del coste total del suministro y los servicios.
- Beneficio industrial:

  Se considera un beneficio industrial del 9% del coste total del suministro y servicios.

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.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

Así pues, la estimación de costes de personal a partir de dicho convenio, y en función de la dedicación del personal asignado a la ejecución del contrato es:

Para la **instalación avanzada**, prevista su realización a lo largo de 1 mes:

Costes de personal (€)							
Perfiles	***Dedicación***	***Salario según convenio***	Especialización tecnológica (XX%)[1]	***Salario anual***	***Coste anual según dedicación***	***Coste personal contrato (1M)***	***Coste personal contrato con Seguridad Social 30%***
CONSULTOR IoT (3-B-I) (1 persona)	33%	27.985,64	74,91%	48.951,05	16.153,85	1.346,15	1.750,00
TÉCNICO DE SISTEMAS Experto (3-B-I) (1 persona)	100%	27.985,64	73,17%	48.461,54	48.461,54	4.038,46	5.250,00
						Total (1M):	**7.000,00**

Para el **soporte y mantenimiento** durante 5 años:

Costes de personal							
Perfiles	***Dedicación***	***Salario según convenio***	***Especialización tecnológica (%)***	***Salario anual***	***Coste anual según dedicación***	***Coste personal contrato (5A)***	***Coste personal contrato con Seguridad Social 30%***
TÉCNICO DE SISTEMAS (3-B-II) (1 persona)	10%	27.147,12	36,01%	36.923,08	3.692,31	18.461,54	24.000,00
						Total (5A):	**24.000,00**

Total Costes de Personal (1M+5A):	**31.000,00**

Si bien resulta de aplicación el Convenio sectorial, en el presente servicio se requiere una cualificación superior debido a la antigüedad requerida de los perfiles definidos, la complejidad inherente a la tecnología específica y en base a las tarifas de mercado manejadas para la estimación del coste de proyecto.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

4.3 TRAMITACIÓN DEL EXPEDIENTE (A EFECTOS PRESUPUESTARIOS)

☒ Ordinaria.

☐ Anticipada:

Se hace constar que el plazo de ejecución comenzará a partir del *01/05/2024*, o de la fecha de confirmación del contrato si ésta fuera posterior, y que la adjudicación del contrato queda sometida a la condición suspensiva de existencia de crédito adecuado y suficiente para financiar las obligaciones derivadas del contrato en el ejercicio correspondiente, de acuerdo con el artículo 117.2 de la LCSP y la normativa contable de aplicación.

4.4 MODIFICACIÓN DEL CONTRATO ESPECÍFICO

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

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

Serán de aplicación las siguientes condiciones:

***NO APLICA*

- Circunstancias admitidas para modificar el contrato específico[6]:
  - …

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 **497.000,00 euros**, según el siguiente desglose:

Valor estimado	Importe (€)
Importe total de la prestación, sin IVA	497.000,00
Importe máximo por modificación prevista, sin IVA	n/a
TOTAL	497.000,00

[6] Entre las circunstancias que se pueden señalar deben precisarse las admitidas en el apartado 27.17 del PCAP del SDA 24/2022.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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.

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

☐ Sí.

☒ No.

En caso afirmativo, se indicará la relación detallada de dichos bienes, con expresión de marca y modelo y part number. Se permitirá el acceso a los mismos a efectos de su valoración.

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: calle Pedro Justo Dorado Dellmans, 11, 28040 MADRID
- Correo electrónico: emi.serrano@csn.es
- Teléfono: 913460270
- Fax: Haga clic o pulse aquí para escribir texto.

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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 PONDERACIÓN[7]

7.1 PONDERACIÓN DE LOS CRITERIOS DE ADJUDICACIÓN

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

Criterio de ahorro o eficiencia energética	Precio	Otros criterios evaluables mediante fórmula
10	*90*	*n.a.*

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

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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 y también si se quiere dar preponderancia en la adjudicación al precio del contrato, aunque todos los criterios sean evaluables mediante fórmula):

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

Donde:

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

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

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

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

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

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

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

Donde:

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

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

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

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

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

7.3 OTROS CRITERIOS EVALUABLES AUTOMÁTICAMENTE MEDIANTE FÓRMULAS, DISTINTOS AL PRECIO

7.3.1 Criterios relativos al consumo energético de los equipos o su eficiencia energética

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Se debe incluir en este apartado el criterio o criterios de valoración correspondientes al mínimo del 5% obligatorio tal y como se define en el PCAP.

CRITERIO	PUNTOS	FÓRMULA DE VALORACIÓ
Criterio eficiencia energética: • Consumo eléctrico medio. Se utilizará el valor de consumo eléctrico medio (Power Supply) indicado en la ficha técnica	**10**	*Minimizar*

7.3.2 Criterios evaluables automáticamente mediante fórmulas

No se considera ningún otro criterio aparte del relativo a consumo energético

7.3.3 Fórmulas para la evaluación automática de los criterios

Función **Maximizar**:

$$C_i = P \cdot \frac{X_i}{X_{máx}}$$

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;
- $X_{máx}$ 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**:

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

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;
- $X_{mín}$ 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;
- $X_{máx}$ es el valor máximo ofertado por los licitadores en el criterio C.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

7.4.2 Método de valoración y documentación

En este apartado se deberá especificar para cada criterio el método de valoración:

- *los aspectos que se valorarán (sólo se podrá puntuar en base a los aspectos que aquí se indiquen),*
- *la documentación que se considerará y*
- *el baremo que se aplicará para valorar cada aspecto.*

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.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

- A la condición anterior, 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: *1%.*

  ☐ Cuando la puntuación conjunta de todos los criterios de los apartados 7.3 y 7.4 se encuentre por encima del siguiente umbral, con respecto a la media la puntuación de todas las ofertas en estos criterios: *indicar % o importe*.

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:

1. A ofertar únicamente productos con distribución comercial, no pudiendo aplicar precios superiores a los de mercado conforme a las condiciones del apartado 17.2 b) del PCAP, y que satisfagan las prestaciones de la garantía obligatoria del fabricante previstas en el apartado III.6 del PPT.
2. 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.
3. Las obligaciones referidas a la protección de datos personales, en los términos previstos en la cláusula 27.5.6 apartado 2 del PCAP.
4. La obligación de confidencialidad del apartado 27.5.8 del PCAP.
5. Las obligaciones establecidas en el apartado 27.5.9 del PCAP respecto al personal laboral.
6. A distribuir únicamente equipamientos que cumplan lo previsto en el apartado III.3 del PPT.
7. 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:

   (X) No existen tareas críticas que no puedan ser subcontratadas en el presente contrato específico.

   (Indicar, si las hay, las tareas críticas que no pueden ser subcontratadas):
   - *Tarea crítica 1*
   - *Tarea crítica 2*
   - *…*
8. 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.
9. 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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

comunicaciones y responsabilizándose de la gestión de la prestación por parte de la empresa adjudicataria.

9.2 OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO

*** NO APLICA ***

9.3 OBLIGACIONES DE SEGURIDAD EN CUMPLIMIENTO DEL ENS

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

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

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

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

10 PAGO Y FACTURACIÓN

10.1 PAGO DEL PRECIO

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

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

☒ A la recepción del servicio, tras su cumplimiento a satisfacción de la Administración.

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

☐ Mensualmente.

☐ Trimestralmente, considerando los siguientes períodos trimestrales:

Período 1: 1-enero a 31-marzo

Período 2: 1-abril a 30-junio

Período 3: 1-julio a 30-septiembre

Período 4: 1-octubre a 31-diciembre

☒ Otra: Anual, al inicio de cada periodo anual de garantía a partir de la fecha de puesta en servicio

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): EA0046348 (Subdirección de Tecnologías de la Información).
- Órgano gestor (DIR3): EA0046348 (Subdirección de Tecnologías de la Información)
- Unidad tramitadora (DIR3): EA0046347 (Subdirección de Personal y Administración)
- Órgano administrativo con competencias en materia de contabilidad pública (DIR3): EA0046347 (Subdirección de Personal y Administración)

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

- Campo <*FileReference*>: SDA 24/2022.
- Campo <*Receiver transaction reference*>: código del contrato específico.

☐ Organismo adherido al Sistema Estatal de Contratación Centralizada.

11 GARANTÍA DE LOS BIENES

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Esta garantía, denominada **garantía obligatoria del adjudicatario**, se ajustará a lo descrito en el apartado III.7 del PPT y tendrá una duración de 2 años independientemente del periodo de **garantía obligatoria del fabricante** del apartado III.6 del PPT, que será de 3 años o un plazo superior (hasta 5 años) según lo previsto en el documento de invitación (Anexo I.3) o el ofrecido por el adjudicatario, en su caso.

En caso de haberse solicitado en el apartado 2.2, a la anterior garantía obligatoria del adjudicatario, será obligatoria una **garantía extendida del adjudicatario** con la cobertura del apartado III.8 del PPT, concretada en el **Anexo V** de este documento, cuya duración se extenderá durante todo el periodo de garantía obligatoria del fabricante de los bienes.

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

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

12 PENALIDADES

12.1 PENALIDADES FIJADAS EN EL SISTEMA DINÁMICO DE ADQUISICIÓN

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

	Valor fijado en el SDA	**Valor fijado en el contrato específico**	**Fórmula de cálculo**
Incumplimiento de las condiciones especiales de ejecución, excepto las relativas a subcontratación.	2% de la facturación del periodo	NO APLICA	Apartado 12.2
Incumplimiento de los ANS.	2% de la facturación del periodo	NO APLICA	Según ANS.
Incumplimiento de los compromisos de adscripción de medios.	2% de la facturación del periodo	NO APLICA	Apartado 12.2
Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas.	2% de la facturación del periodo	NO APLICA	Apartado 12.2
Demora en el cumplimiento del plazo total del contrato	Resolución / 0,60 euros por cada día y 1.000 euros del precio del contrato, IVA excluido		Valor fijado en el SDA

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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 en cumplimiento del ENS, o de los requisitos de seguridad para la protección de datos personales 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
  - lo indicado en SDA
- Incumplimiento de los ANS:
  - lo indicado en SDA
- Incumplimiento de los compromisos de adscripción de medios
  - lo indicado en SDA
- Incumplimiento de las condiciones ofertadas en los criterios de adjudicación y que fueron valoradas
  - lo indicado en SDA

12.2 FÓRMULA PARA LA APLICACIÓN DE PENALIDADES

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

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

Donde:

a) I_P es el importe de la penalidad a aplicar
b) I_F es el importe del periodo de facturación, antes de la aplicación de ninguna penalidad
c) 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.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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 PLACSP[8] u otra plataforma de contratación a disposición del organismo.

Las ofertas deberán firmarse electrónicamente por el representante legal de la empresa[9].

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

La oferta económica deberá incluir, al menos, la información en el modelo de oferta disponible en el Portal de Contratación Centralizada para el SDA 24/2022, en la siguiente dirección: https://contrataccioncentralizada.gob.es/documents/11614/217411/Modelos+de+Oferta+SDA24_2022.zip/8fd8b709-6ed2-4581-9bd2-f88f0940780a

Junto con la invitación, el organismo destinatario podrá adjuntar un modelo de oferta económica más detallado, que complemente la información exigida en el citado modelo de oferta.

La oferta técnica deberá contener la siguiente documentación:

- Relación de los equipos y/o programas que se ofertan
- La información de los requisitos mínimos de los productos o referencias a las fichas técnicas o catálogos que permitan acreditar los criterios automáticos:
    - Para la comprobación de la oferta técnica, la misma expondrá su solución técnica, mediante una exposición del cumplimiento requisito a requisito de los expuestos en Anexos I y II, haciendo referencia a documentación oficial del fabricante o equivalente.

- La información necesaria para la evaluación de los criterios automáticos de la instalación avanzada y/o soporte y su acreditación, siguientes:
    - Consumo eléctrico homologado de los equipos

- Si la oferta incluye equipos y/o programas que forman parte de la arquitectura de seguridad del organismo **se deberá incluir la acreditación de los requisitos de seguridad** exigidos por cualquiera de los medios descritos en el apartado III.2.2 o III.2.3 del PPT, según corresponda. La falta de acreditación será motivo de exclusión de la oferta.

[8] Plataforma de Contratación del Sector Público: https://contrataciondelestado.es/wps/portal/guiasAyuda

[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.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

-

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

EN LO QUE ESTE DOCUMENTO DE INVITACIÓN SE OPONGA A LOS PLIEGOS DEL SISTEMA DINÁMICO DE ADQUISICIÓN, 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): Subdirector de Tecnologías de la Información.

Firmado electrónicamente (nombre y apellidos): **Javier López Orcajo**

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

ANEXO I PRESCRIPCIONES TÉCNICAS

I.1. REQUISITOS FUNCIONALES DE LOS SUMINISTROS

Antecedentes para la renovación de equipos

El Consejo de Seguridad Nuclear (en adelante CSN) precisa renovar sus cortafuegos externos para la adecuada gestión de interfaces de acceso, seguridad de las redes LAN e Internet de alta velocidad, protegiendo todo el tráfico que circula por dichas líneas, incluido el cifrado, con capacidades de gestión y prevención de amenazas. Así mismo, necesita proteger los dispositivos IoT (Internet de las Cosas) de amenazas desconocidas, en función de recomendaciones de políticas automáticas.

Actualmente el CSN cuenta con dos equipos PA-3020 cuyo fin de soporte de hardware (EOSH) finaliza a lo largo de 2024. El soporte actual de las licencias de dichos equipos finaliza el 30 de abril.

La relación de licencias que CSN tiene contratado el soporte con los equipos actuales son:

Licencia o suscripción
Threat prevention subscription renewal for devices in HA pair, PA-3020
PANDB URL filtering subscription renewal for devices in HA pair, PA-3020
WildFire subscription renewal for devices in HA pair, PA-3020
Partner enabled premium support year 1 renewal, PA-3020

Por otra parte, CSN dispone de 2 equipos de cortafuegos internos de tecnología FORTINET.

Equipamiento a suministrar

- 2 equipos FW (cortafuegos) para reemplazar los 2 PA-3020 actuales
- Licencias equivalentes a las actuales
- Transceivers y cableado necesario para llevar a cabo el reemplazo en las condiciones requeridas, al menos:
    - 2 SFP de 25 Gb.
    - 20 SFP de 10 Gb.

[RT-RH] Requerimientos físicos/hardware

[RT-RH-1] Puertos y gestión E/S

Puertos necesarios (cada equipo):

- 12 puertos de 1/2.5/5 /10 Gb.
- 10 puertos SFP/SFP+ de 1/10 GB.
- 2 puertos SFP 28 de 25 GB

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Gestión E/S:

- (1) puerto de gestión fuera de banda 100/1000
- (2) puertos 100/1000 de alta disponibilidad, (1) puerto SFP+ de 10 Gb de alta disponibilidad
- (1) puerto de consola RJ-45, (1) micro-USB

[RT-RH-2] Capacidad de almacenamiento: 480 GB en disco SSD

[RT-RH-3] Conexión eléctrica

Fuente de alimentación Redundante

BTU/h máximo: 650

Tensión de entrada (frecuencia de entrada) CA: 100–240 V CA (50-60 Hz)

Consumo máximo de corriente CA: 1,9 A a 100 V CA, 0,8 A a 240 V CA

[RT-RH-4] Tiempo medio entre fallos (MTBF): 22 años

[RT-RH-5] Seguridad/Certificaciones:

cTUVus, CB ; Clase A de FCC; Clase A de CE; Clase A de VCCI

[RT-RH-6] Entorno físico:

- Temperatura de funcionamiento: de 0 °C a 50 °C
- Temperatura de almacenamiento: de -20 °C a 70 °C
- Tolerancia a la humedad: del 10 % al 90 %
- Altura máxima: 3048 m (10.000 pies)
- Flujo de aire: de delante a atrás

[RT-LIC] <u>Requerimientos sobre licencias</u>

Las licencias que deberán incorporar los equipos:

- **[RT-LIC-1] Advanced threat prevention**:
    - para detener las amenazas conocidas de exploits, malware, spyware y comando y control, utilizando la prevención de ataques de día cero. Que prevenga del 60 % o más de ataques por inyección desconocidos y un mínimo de 48 % más de tráfico de comando y control, con las soluciones IPS tradicionales.
- **[RT-LIC-2] Advanced URL Filtering**:
    - que garantice el acceso seguro a internet y evite un mínimo de 40 % o más de ataques basados en la web, con el primer sistema de prevención, en tiempo real, de amenazas conocidas y desconocidas del sector. Que detenga al menos un 88 % de las URL maliciosas.
- **[RT-LIC-3] Advanced WildFire:**

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

- que garantice la seguridad de los archivos, previniendo automáticamente el malware conocido, desconocido y muy evasivo con una rapidez al menos 60 veces superior a los actuales, gracias al mayor motor de inteligencia sobre amenazas.

- **[RT-LIC-4] IoT Security**:

  - protege todos los dispositivos inteligentes e implementa un modelo de seguridad Zero Trust (confianza cero). Permite descubrir los ángulos muertos de las soluciones implementadas de IoT:

    - Control de acceso a la red
    - Gestión de activos
    - Gestión de vulnerabilidades
    - Detección y respuesta
    - Gestión de redes

[RT-CG] Características generales de los equipos a suministrar

[RT-CG-1] La tecnología de los cortafuegos requeridos no puede ser la misma que la de los cortafuegos internos ya en uso (Fortinet), como se indica en las guías de buenas prácticas que CCN describe en sus guías de seguridad perimetral (CCN-STIC-408, CCN-STIC-811), para reducir la posibilidad de que una vulnerabilidad en uno de ellos se reproduzca automáticamente en el otro.

[RT-CG-2] Cortafuegos de nueva generación de aprendizaje automático que prevenga ataques sin firmas de forma integrada y capacidad de identificar y detener ataques de phising no conocidos. Que detecte y recomiende políticas, analizando el comportamiento en la nube e integrado de forma nativa en los equipos.

[RT-CG-3] Inspección de tráfico de capa 7, identificando y clasificando las aplicaciones en cualquier puerto, protocolo, técnicas de evasión o tipo de cifrado (TLS o SSL). Tome decisiones de habilitación segura de políticas: permitiendo, denegando, programando, inspeccionando o aplicando catalogación del tráfico. Tenga la posibilidad de crear etiquetas App-ID personalizadas, propiedad de la organización. Identifique los datos de carga útil de una aplicación (archivos, patrones de datos, etc) para bloquear archivos maliciosos y evite intentos de exfiltración de datos.

[RT-CG-4] Permita aplicar políticas de seguridad a los usuarios, independientemente de la ubicación en que se encuentren, adaptando éstas a la actividad realizada. Para ello, deberá poder integrarse con otra infraestructura del CSN como Wifi, VPN, ADs, etc. Permita, a su vez, definir grupos de usuarios dinámicos (DUG) para poder adoptar medidas de seguridad temporales, sin aplicar cambios a los directorios de usuarios. Aplicación de políticas, independientemente de la ubicación de los dispositivos (viaje, casa, trabajo) y del tipo de dispositivo (Windows, Linux, MacOS, IOS, Android, VDI …). Incluya MFA en la capa de red de cualquier aplicación, salvaguardando las credenciales e impidiendo que éstas se filtren en webs de terceros. Proporcionar medidas de seguridad dinámicas, basadas en el comportamiento de los usuarios, imponiendo restricciones a aquellos que se consideren sospechosos o malintencionados. Autentique y autorice a los usuarios, independientemente de su ubicación.

[RT-CG-5] Impida ocultar actividad maliciosa en el tráfico cifrado, inspeccionando y aplicando políticas (TSL/SSL) tanto en tráfico entrante como saliente, incluidos los protocolos TLS 1.3 y HTTP/2. Visibilidad total del tráfico transmitido a través del protocolo TLS. Controlar TLSs obsoletos, con tipo de cifrados

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

poco seguros y certificados configurados de forma incorrecta, mitigando riesgos innecesarios. Ayuda en la implementación del descifrado para permitir utilizar logs que ayuden en la resolución de problemas. Permitir crear copias del tráfico descifrado para su envío a herramientas de recopilación de tráfico y así poder realizar análisis forense. Permita desviar tráfico (cifrado, descifrado, …) a herramientas de seguridad de terceros.

[RT-CG-6] Deberá contar con la funcionalidad SD-WAN.

[RT-RDTO] <u>Rendimiento</u>

[RT-RDTO-1] El rendimiento de los equipos tiene que cumplir con los siguientes valores:

Rendimiento del cortafuegos (HTTP/ combinación de aplicaciones de 64KB*)	20,8/16,9 Gb/s
Rendimiento de Threat Prevention (HTTP/ combinación de aplicaciones**)	7,6/8,7 Gb/s
Rendimiento de VPN Ipsec***	9,9 Gb/s
Número máximo de sesiones	2 mill.
Nuevas sesiones por segundo****	205.000
Sistemas virtuales (base/máx)*****	1/11

[RT-RDTO-2] Se ha de garantizar que el firewall ofertado, no sufrirá degradación conforme se vayan habilitando perfiles de seguridad relacionados con la protección, es decir tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc) como frente a amenazas desconocidas (Sandboxing), de forma que sea predecible el impacto en el rendimiento de la solución en la activación progresiva de estas funciones de seguridad, independientemente del número de ellas.

Se reserva el derecho de realizar un test de rendimiento de la plataforma ofertada, con todas las funciones de seguridad disponibles en la plataforma, independientemente de los incluidos en la propuesta, aplicados sobre el tráfico real existente en el datacenter a proteger.

[RT-RDTO-3] La arquitectura hardware de la plataforma deberá permitir la aplicación paralela de diferentes módulos de seguridad, asegurando una sola inspección por cada paquete. No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering,…).

[RT-RDTO-4] La arquitectura hardware habrá de proveer de procesadores específicos para el descifrado de tráfico

[RT-GA] <u>Gestión y Administración</u>

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión y administración de la propia plataforma, entendiéndose como funcionalidades mínimas a cumplir:

[RT-GA-1] Procesadores y memoria dedicados para los planos control y datos, para asegurar el acceso a la gestión en caso de saturación del plano de datos.

[RT-GA-2] Gestión completa del firewall desde el propio dispositivo sin necesidad de appliance externos, es decir, se podrá realizar políticas de seguridad, obtención de informes, etc. desde el propio firewall.

[RT-GA-3] Gestión de políticas, objetos, interfaces, etc., desde la propia interfaz del Firewall, sin necesidad de instalar otros componentes.

[RT-GA-4] Gestión y administración por medio de interfaz web y a través de línea de comandos, debiendo existir la posibilidad de utilizar API XML para configuración de ciertas funcionalidades.

[RT-GA-5] Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.

[RT-GA-6] Posibilidad de aplicar cambios en configuración pendientes, visualizar dichos cambios antes de aplicarlos, así como validarlos antes de aplicarlos en configuración. Se debe también tener la posibilidad de almacenar diferentes versiones de configuraciones, así como descartar cambios en configuración realizados.

[RT-GA-7] Envío de logs vía SYSLOG, FTP, SCP y TFTP para retención y posterior tratamiento, con posibilidad de envío de logs selectivos según niveles de severidad y también según atributos como por ejemplo los tipos de amenaza.

[RT-GA-8] Soporte SNMP incluyendo la posibilidad de obtener estadísticas relativas a los procesos de recolección de logs y del estado de salud de las funciones de alta disponibilidad.

[RT-GA-9] Debe existir la posibilidad, aunque no fuera objeto de este contrato, de disponer una consola de gestión única para firewalls físicos, virtuales, o en cloud, para reducir los costes de operación y la curva de aprendizaje.

[RT-RED] <u>Funcionalidad de red</u>

Cada firewall ofertado deberá tener las siguientes características técnicas de red básicas:

[RT-RED-1] Los interfaces del firewall deben soportar los siguientes modos de funcionamiento:

- Modo TAP para monitorizar tráfico de forma pasiva a través de puertos mirror.
- Modo transparente para inspección de tráfico en el flujo de datos y despliegues “in-line”.
- Modo layer 2 o switching.
- Modo layer 3 o routing.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Y debe ofrecer la posibilidad de utilizar varios interfaces trabajando en diferente modo, al mismo tiempo y en la misma instancia, para poder abarcar despliegues híbridos.

[RT-RED-2] VLAN**:**
Soporte de IEEE 802.1Q y agregación de interfaces mediante 802.1ad soportando hasta 8 grupos de agregación con 8 interfaces cada grupo.

- Etiquetas VLAN 802.1Q por dispositivo/interfaz: 4094/4094
- Interfaces agregadas (802.3ad), LACP

[RT-RED-3] Enrutamiento**:**

- Soporte de protocolos dinámicos de routing RIP, OSPF *v2/v3* y BGP4 con reinicio correcto, así como routing estático,
- Reenvío basado en políticas
- Protocolo punto a punto sobre Ethernet (PPPoE)
- Multidifusión: PIM-SM, PIM-SSM, IGMP versiones 1, 2 y 3
- Detección de reenvío bidireccional (BFD)

[RT-RED-4] Enrutamiento avanzado**:**

El equipo cortafuegos debe disponer de un motor avanzado de routing, que simplifica las operaciones con configuraciones basados en estándar.

- Se deben permitir la configuración de perfiles para cada protocolo y el filtrado granular de cada perfil para multiples routers lógicos y sistemas virtuales.
- Se debe permitir la redistribución de rutas con perfiles de redistribución.
- Capacidad de realizar policy base routing en base a IP o red de origen, o también basado en usuarios/grupos o por tipo de aplicación
- Se debe permitir grupos de peers BGP que hereden configuraciones.
- Se debe dar soporte a rutas estáticas BGP, MP-BGP, OSPFv2, OSPFv3, RIPv2, IPv4 multicast routing, BFD, redistribución, filtrado de rutas en el RUB, access lists, prefix lists y route maps

[RT-RED-5] Capacidad de detección de fallos bidireccional entre Firewall y Router para aplicar a protocolos de routing dinámicos o rutas estáticas.

[RT-RED-6] Traducción de direcciones de red

- Soporte de DHCP, NAT y PAT.
- Modos de NAT (IPv4): IP estática, IP dinámica, IP dinámica y puerto (traducción de direcciones de puertos)
- NAT64, NPTv6
- Funciones NAT adicionales: reserva de IP dinámica, IP dinámica optimizable y sobresuscripción de puertos

[RT-RED-7] Alta disponibilidad:

- Modos: activo/activo, activo/pasivo, clúster de alta disponibilidad
- Detección de errores: supervisión de rutas y supervisión de interfaces

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

[RT-RED-8] Capacidad de realizar VPN “Site to Site” o “SSL VPN”

[RT-RED-9] VPN IPsec

- Intercambio de claves: clave manual, IKEv1 e IKEv2 (clave precompartida, autenticación basada en certificados)
- Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)
- Autenticación: MD5, SHA-1, SHA-256, SHA-384 y SHA-512

[RT-IDUS] <u>Integración e identificación de usuarios.</u>

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión e identificación de usuarios, entendiéndose como funcionalidades mínimas a cumplir:

[RT-IDUS-1] Posibilidad de aplicar políticas basadas en usuarios y grupos en vez de por IP.

[RT-IDUS-2] Integración con sistemas de directorios para obtención de usuarios y grupos, incluyendo Microsoft Active Directory, Novell eDirectory y Sun ONE Directory.

[RT-IDUS-3] Posibilidad de integración con sistemas multiusuario como Citrix o Microsoft Terminal Server para la identificación unívoca de los usuarios para el tráfico generado desde estos sistemas.

[RT-IDUS-4] Capacidad de analizar mensajes de syslog con información de login y logout para identificación de usuarios.

[RT-IDUS-5] Posibilidad de inyectar usuarios mediante aplicaciones de terceros a través de API XML.

[RT-IDUS-6] Capacidad de poder identificar usuarios mediante portal de autenticación propio haciendo uso de protocolos como Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.

[RT-SEG] <u>Características generales de seguridad.</u>

Los equipos ofertados deben cumplir con los siguientes requerimientos mínimos en cuanto a funcionalidades relativas a seguridad:

[RT-SEG-1] Posibilidad de agrupar interfaces del propio firewall en conjuntos independientes formando zonas, de forma que las políticas de seguridad se definan por zonas pudiendo incluir en las mismas políticas varias zonas origen para el análisis de tráfico y procesado de reglas de seguridad, así como la posibilidad de crear múltiples reglas de seguridad entre zonas origen y destino o incluir cualquier zona origen o destino de tráfico en dichas reglas.

[RT-SEG-2] Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 3600 identificadas así como la identificación de subfunciones dentro de una aplicación como por ejemplo “compartir escritorio de webex”, “chat dentro de webex”, “transferencia de ficheros en webex”, etc.

[RT-SEG-3] Posibilidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.

[RT-SEG-4] Posibilidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.

[RT-SEG-5] Posibilidad de identificar aplicaciones propietarias que usen los protocolos HTTP y TCP.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

[RT-SEG-6] Posibilidad de identificar aplicaciones que vayan bajo túneles encriptados SSL.

[RT-SEG-7] Capacidad de descifrar tráfico SSH y detectar aplicaciones no legítimas sobre este protocolo.

[RT-SEG-8] Posibilidad de crear reglas de calidad de servicio según las aplicaciones que se usen en el tráfico, y los usuarios o grupos de usuarios que lo generen.

[RT-SEG-9] Posibilidad de aplicar diferentes perfiles de seguridad (IPS, Antivirus, Antispyware, Sandboxing, etc) para diferentes aplicaciones que funcionen por el mismo puerto.

[RT-SEG-10] Posibilidad de aplicar políticas de NAT de forma independiente a las políticas de seguridad ante vulnerabilidades y de protección de la red interna.

[RT-SEG-11] Posibilidad de habilitar todas las funciones de seguridad que ofrezca el equipo, sin penalización en rendimiento dependiendo del número de ellas habilitadas.

[RT-SEG-12] Capacidad de requerir autenticación de múltiple factor en el acceso a cualquier servicio del datacenter para verificar la identidad real del usuario, independientemente de la aplicación utilizada. Deberá permitir la integración de forma nativa con soluciones como Okta, Ping Identity, Duo v2, RSA SecureID Access, y en general con cualquier otro vía Radius o SAML.

[RT-SEG-13] Posibilidad de descifrar tráfico cifrado y enviarlo en claro a otras soluciones para realización de sus funciones, y recibirlo nuevamente después para su envío a destino previa aplicación de las políticas de seguridad que correspondan en el firewall.

[RT-SEG-14] Utilización de motores propios de inspección para los servicios de seguridad (Antivirus, IPS, URL Filtering, Antimalware, etc) y no de terceros.

[RT-SEG-15] NGFW con motores basados en Machine Learning entrenados en la nube para proporcionar protección en tiempo real de amenazas desconocidas, URLs maliciosas, DNS, y seguridad IoT.

[RT-SEG-16] Integrar machine learning (ML) en el núcleo del firewall a fin de proporcionar una prevención de ataques sin firma internos para los ataques basados en archivos, mientras identifica y detiene de inmediato los intentos de phishing nunca antes vistos.

[RT-SEG-17] Posibilidad de importar reglas de Snort y Suricata como firmas de IPS del Firewall, ya sea a través del Firewall o a través de la consola de gestión.

Protección ante ataques denegación servicio.

[RT-SEG-18] Los cortafuegos ofertados deben contar con medidas de protección ante ataques de Denegación de Servicios de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las direcciones ip origen y destino a inspeccionar o el usuario o grupo de usuarios interno de la red que puede estar originando el ataque.

Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

[RT-VUL] Protección ante vulnerabilidades.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Los cortafuegos ofertados deben contar con la posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente, debiendo cumplir con las siguientes funcionalidades:

[RT-VUL-1] Se debe poder aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de Internet sin incurrir en latencia superior a 1 milisegundo para no penalizar la sensación del usuario, efectuando el análisis en una única pasada para todo tipo de amenazas.

[RT-VUL-2] En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas.

[RT-VUL-3] Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades especificando si son vulnerabilidades que aplican a los clientes, los servidores o a ambos indistintamente.

[RT-VUL-4] Las vulnerabilidades deben estar categorizadas por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.

[RT-VUL-5] Se debe poder permitir usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.

[RT-VUL-6] Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.

[RT-AUF] <u>FILTRADO DE URL. (URL filtering)</u>

Los equipos ofertados deben tener la posibilidad de filtrar la navegación http o https según la URL que se desea visitar basándose en diferentes criterios:

[RT-AUF-1] Posibilidad de definir manualmente listas estáticas de URL o de IP permitidas y no permitidas para la navegación, con posibilidad de definir para las no permitidas la acción a realizar (bloquear, permitir pero advertir, generar solamente un log, etc).

[RT-AUF-2] Permitir la navegación basándose en categorías de URL, siendo dichas categorías actualizadas periódicamente a través de un servicio en la nube que permita al menos categorías de URL como “malware”, “phishing”, “command-and-control”, “hacking”, etc.

[RT-AUF-3] Posibilidad de incluir listas dinámicas, de forma que los equipos puedan ser configurados para que de forma periódica consulten fuentes de inteligencia propios o de terceros con IoCs maliciosos, y permita automatizar la denegación del tráfico hacia/desde estos IoCs en la política del firewall. Se valorará positivamente que el fabricante ofrezca listas de IPs maliciosas que se actualicen y mantengan automáticamente.

[RT-AUF-4] Posibilidad de detectar el robo y envío de credenciales corporativas (usuarios y password de la red corporativa) hacia las webs que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales en función de las categorías de web visitadas.

[RT-AUF-5] Se deberá dotar al firewall de modelos de Machine Learning para poder detectar Inline, en el propio firewall de páginas de phishing, así como de scripts Javascript maliciosos.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

[RT-AUF-6] Se deberá disponer de mecanismos de Machine Learning en nube para categorizar páginas web que no estén categorizadas por el sistema del filtrado de URL general.

[RT-AUF-7] Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

[RT-DEC] Detección de equipos comprometidos en la red

[RT-DEC-1] Los cortafuegos ofrecidos deben tener la capacidad mediante firmas de detectar posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante log este tipo de tráfico.

Entre las acciones posibles, se debe tener la capacidad de habilitar mecanismos de DNS sinkholing que permitan interceptar las peticiones de resolución de dominios realizadas desde servidores propios DNS internos a la red o hacia servidores DNS externos de forma que se identifique los equipos internos comprometidos por algún tipo de malware.

[RT-ATP] Funcionalidades Antivirus (Threat Prevention)

Los cortafuegos propuestos deben tener la capacidad de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet a red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

[RT-ATP-1] Se debe poder aplicar políticas que permitan aplicar el motor de antivirus sobre protocolos como ftp, http, imap, pop3, smb o smtp, definiendo para cada uno de estos protocolos la acción a realizar (permitir los ficheros, descartar los ficheros, desconectar la sesión o registrar mediante logs) ante la detección del fichero malicioso por el motor de antivirus, adicionalmente, se debe poder tener la posibilidad de enviar el fichero que se inspecciona a un servicio en Internet que permita el análisis de dicho contenido y emita un veredicto en caso de que el fichero sea malicioso que permita realizar al cortafuegos las acciones oportunas.

[RT-ATP-2] Los cortafuegos deben permitir la aplicación de políticas de antivirus de forma granular, permitiendo por ejemplo la aplicación de dichas políticas a ciertos usuarios de determinados grupos o a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

[RT-ATP-3] El módulo de Antimalware deberá de disponer de un motor de análisis estático basado en algoritmos de Machine Learning que permitan identificar muestras maliciosas desconocidas en tiempo real sin necesidad de tener que esperar al veredicto del módulo de Sandboxing.

[RT-AWF] Tecnología de sandboxing (Wildfire)

[RT-AWF-1] Los cortafuegos propuestos deben tener la capacidad de disponer de un servicio en la nube capaz de analizar ficheros de tipo desconocido o enlaces URL recibidos en correos electrónicos, de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

[RT-AWF-2] El servicio en la nube será capaz de analizar los siguientes tipos de ficheros: paquetes de aplicaciones Android, ficheros flash, applets java, ficheros de Microsoft office, ficheros ejecutables con

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

formato PE incluyendo dll, ficheros pdf y enlaces HTTP y HTTPS incluidos en correos electrónicos recibidos por SMTP y POP3.

[RT-AWF-3] El análisis realizado por este servicio en la nube en caso de que la muestra enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad deberá generar las firmas apropiadas en un plazo máximo de 5 minutos que se utilizarán para actualizar los motores propios de antivirus y filtrado URL de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas por dichos firewalls.

[RT-AWF-4] Además, el firewall también se aprovechará, en el mismo plazo de tiempo, de la inteligencia generada para cualquier muestra analizada en dicho servicio incluso procedente de otros clientes u otras fuentes externas.

[RT-AWF-5] Será valorable la compartición de esta inteligencia con alguna solución de puesto de trabajo para que en ese plazo máximo de 5 minutos, también lo desconocido sea convertido en conocido en el contexto de protección en el puesto.

[RT-AWF-6] Los firewalls deben tener la capacidad de enviar también al servicio de sandboxing en la nube no solamente aquellos ficheros de tipo sospechoso sino aquellos que hayan sido bloqueados por su propio sistema de firmas, con objeto de poder analizar variantes de malware e incorporar esas variantes al sistema de firmas de los propios motores del equipo. Además, se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

[RT-AWF-7] Para satisfacer requerimientos regulatorios de privacidad de datos a nivel europeo como GDPR, este servicio en la nube debe estar disponible en una nube regional en la Unión Europea de tal forma que las muestras enviadas a esta nube permanecerían dentro de sus fronteras.

[RT-AWF-8] Además, este servicio en la nube habrá de estar basado en un hipervisor específicamente diseñado por el fabricante y contará con la posibilidad de detonación en hardware físico para aquellas muestras altamente evasivas en entornos de sandbox virtuales.

[RT-AWF-9] Capacidad para detectar y bloquear variantes maliciosas de los ejecutables y los scripts de PowerShell en tiempo real mediante el aprendizaje automático (ML) en el propio firewall.

[RT-IOT] <u>Identificación de dispositivos (IoT)</u>

[RT-IOT-1] Se deberá poder obtener información de los dispositivos sin equipamiento adicional, únicamente con el tráfico que se observe en el firewall. Esta información será, entre otros:

- Información del fabricante del dispositivo
- Tipo de dispositivo
- Versión del SO
- IP y MAC
- Tráfico que ha realizado el dispositivo y detección de las aplicaciones
- Vulnerabilidades que pueda tener el dispositivo basado en la información de SO, con el CVE asociado si existe y un Score de riesgo.

[RT-IOT-2] Se deberá poder analizar el comportamiento para evaluar el riesgo del dispositivo, el cumplimiento y la actividad anómala, y prevenir las amenazas conocidas y desconocidas.

[RT-IOT-3] Debe facilitar la adopción de Zero Trust con políticas automatizadas de acceso con privilegios mínimos y se aplicará con un solo clic.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

[RT-IOT-4] Proporcionará recomendaciones de políticas basadas en el comportamiento del perfil del dispositivo en la red local

[RT-IOT-5] Se deberá poder establecer alertas basadas en comportamiento del dispositivo, por ejemplo, se podrá generar una alerta cuando el dispositivo exceda de un tráfico específico en 10 minutos, o detectar que un dispositivo está desconectado más de 1 hora.

[RT-IOT-6] Se podrán generar informes de los dispositivos, como informe de vulnerabilidades o informe de riesgo de los dispositivos

[RT-IOT-7] Deberá ofrecer integración de sistemas externos de forma bidireccional, como gestores de vulnerabilidades (Rapid7, Tenable, Qualys).

Conexión técnica a la nube

[RT-NUB-1] No serán admisibles en ningún caso soluciones de puesta a disposición de activos en la nube. Sólo estará permitida la conexión técnica a la nube de los equipos en los términos descritos en el apartado III.5 del PPT. Los licitadores se comprometen a que los equipos ofertados cumplen con las condiciones y límites definidos para este tipo de conexiones.

Soporte hardware/software

[RT-EOL-1] Los equipos suministrados no deben tener fecha EOL (End-of-Life) anunciada por fabricante a la fecha de entrega de los mismos, garantizando un mínimo de 10 años de soporte hardware.

[RT-EOL-1] El tipo de soporte de fabricante será el equivalente al actual del fabricante actual (PA Premium Support)

I.2. REQUISITOS NO FUNCIONALES DE LOS SUMINISTROS

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

Confidencialidad de los datos de CSN:

Con carácter general el adjudicatario queda expresamente obligado a las obligaciones de protección de la información confidencial que establece el artículo 133, apartado 2, de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público.

La empresa adjudicataria y los miembros del equipo de trabajo, en particular, guardarán secreto profesional sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, quedando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución. Esta obligación no se limitará al tiempo de ejecución del correspondiente contrato, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier información relacionada con el objeto del contrato, sea cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (verbal, escrita,

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

grabada o en cualquier otro medio), que pudiera ser facilitada por el CSN o por cualquier tercero que tenga relaciones contractuales con el organismo, será considerada como "*Información Confidencial*".

I.3. CARACTERÍSTICAS DE LA GARANTÍA OBLIGATORIA DEL FABRICANTE

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

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

Opcionalmente, se pueden exigir en este apartado algunas de las siguientes opciones:

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

☒ Ampliación de horarios de soporte: *24x7*

☐ Reducción de los tiempos de respuesta: Haga clic o pulse aquí para escribir texto.

☐ Reducción de los tiempos de resolución: Haga clic o pulse aquí para escribir texto.

☒ Periodo de garantía superior: 5 años de garantía

☒ Otras condiciones adicionales exigibles al fabricante: modelo "Partner enabled premium support" o equivalente, para dar continuidad al del mantenimiento actual

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

I.4. PERIODO DE VIGENCIA Y MODALIDAD DE LICENCIAMIENTO

El periodo de vigencia del licenciamiento será de 5 años contados a partir del día siguiente a la certificación de la puesta en servicio de los nuevos equipos reemplazando los actuales y con la misma funcionalidad actual (resultante de la instalación avanzada que incluye el contrato).

Se incluirá el mantenimiento de las actuales licencias con los equipos existentes hasta dicha fecha de puesta en servicio, si ésta fuese posterior al vencimiento del contrato de mantenimiento vigente.

Vigencia de las licencias:

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Programa	**Periodo de vigencia del licenciamiento**
Advanced threat prevention for device in HA pair	5 años
Advanced URL Filtering for device in HA pair	5 años
Advanced WildFire for device in HA pair	5 años
IoT Security for device in HA pair	5 años

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

Programa	**Derechos durante la vigencia de las licencias**
Advanced threat prevention Advanced URL Filtering Advanced WildFire IoT Security (for devices in HA pair)	• Derecho de uso: *por equipo* • Derecho de actualización: CSN dispondrá de acceso y descarga ilimitada a las actualizaciones y nuevas versiones software/firmware que formen parte de los equipos, licencias/suscripciones adquiridas en la solución. El contratista, al inicio del contrato, proporcionará las cuentas y datos que habiliten estos accesos. • Derecho de acceso a documentación: CSN dispondrá de acceso y descarga ilimitada a las actualizaciones y nuevas versiones software/firmware que formen parte de los equipos, licencias/suscripciones adquiridas en la solución. El contratista, al inicio del contrato, proporcionará las cuentas y datos que habiliten estos accesos. • Derecho de consulta al fabricante (soporte del fabricante): Soporte general 24x7, según ANSs para incidencias críticas. Para consultas o incidencias de severidad baja: o Horario: *9:00 A 17:00* o Tiempo de respuesta: 5 días laborables • Otros derechos:
	•

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

II.1. SERVICIOS DE INSTALACIÓN AVANZADA DE LOS SUMINISTROS

Alcance

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

La puesta en marcha de los suministros solicitados requiere de una serie de trabajos adicionales a los de instalación básica y que forman parte del objeto del contrato, es decir, se precisan los servicios de instalación avanzada.

Dichos trabajos incluirán lo siguiente, una vez realizada la instalación y configuración básica de los nuevos equipos:

- Preparación

Definición de un **Plan de Implantación** que contemple el estudio de la configuración actual, análisis de las necesidades de CSN, revisión de las opciones de configuración posibles y concluya con la elaboración del correspondiente diseño de arquitectura e implantación, tanto lógica como física. El plan de Implantación debe incluir todas las tareas necesarias desde la entrada del equipamiento hasta su puesta en servicio fina, incluyendo, entre otras, tareas tales como:

- Desembalado de los nuevos equipos, retirada de todas las cajas de embalaje y su reciclaje correspondiente
- Ampliación de los nuevos equipos, con los nuevos módulos (tarjetas, fuentes de alimentación, transceptores etc.)
- Inventariado de los equipos.
- Instalación de los nuevos equipos en los racks que se habiliten para ello.
- Cableado eléctrico y de red
- Peinado y etiquetado de todo el cableado implicado en la instalación de los equipos
- Instalación, configuración y activación del licenciamiento y software en los nuevos equipos
- Incorporación y configuración de los equipos en las herramientas de administración y operación de CSN
- Migración de configuración, reglas y políticas de seguridad desde los equipos actuales a los nuevos, manteniendo totalmente la compatibilidad con las funciones y dispositivos disponibles e integrados con los cortafuegos actuales.
- Configuraciones adicionales a incluir con los nuevos equipos:
    - aquellas relativas a la licencia de IoT Security, integrando con equipamiento que el CSN tiene actualmente en WAN u otros dispositivos.
- Pruebas pre-sustitución de la operatividad de los equipos.
- Sustitución de equipos. Retirada y destrucción o inhabilitación segura de los equipos antiguos.
- Pruebas post instalación de validación.
- Plan de marcha atrás (rollback plan) en caso de detectarse algún comportamiento anómalo de la solución.
- Tests de vulnerabilidades con herramientas al uso para este tipo de dispositivos, una vez puesta en marcha la nueva solución (tipo Rapid7, Nessus, …)

Definición de un **Plan de Pruebas** a ejecutar tras la implantación que valide el correcto funcionamiento del sistema, incluyendo pruebas de vulnerabilidades y el informe final favorable. El resultado de su ejecución será la base principal para certificar la puesta en servicio. Será validado por CSN previo a la ejecución.

- Instalación y configuración

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Instalación y configuración de los equipos, de las licencias que formen parte de la solución y la integración con el resto de la infraestructura corporativa del CSN para su correcto funcionamiento conforme al Plan de Implantación aprobado, incluyendo las características inherentes a la licencia IoT, y manteniendo la compatibilidad con todos los dispositivos de la red de CSN integrados con los cortafuegos.

Se asegurará la mínima interrupción del servicio operativo, por lo que, aunque los trabajos se realizarán principalmente en horario de oficina de CSN, las intervenciones se realizarán en las fechas y horarios autorizados, lo que podría incluir fines de semana y festivos.

Se entregará al final a CSN la documentación técnica soporte de la instalación y configuración realizada.

- Puesta en servicio

Aplicación del Plan de Pruebas (plan validado por CSN previo a la ejecución) para verificar el correcto funcionamiento de la solución implantada.

CSN certificará la instalación si el resultado de la ejecución del Plan de Pruebas es aceptable.

- Transferencia del conocimiento y documentación

Se realizará la transferencia de conocimientos de la nueva tecnología al personal técnico de CSN, acompañada de la documentación técnica de instalación y configuración, así como de la documentación previa actualizada de Plan de Implantación y Diseño arquitectura.

Así mismo se entregará un Manual de Operación y Monitorización con la documentación de las acciones a realizar para los casos más comunes de operación o incidencias. Este manual debe contar necesariamente con un apartado para describir las principales acciones de Monitorización.

Hitos y entregables

Hito	**Descripción del hito y sus entregables**	**Plazo**	**Porcentaje de la prestación**
HITO_01	Preparación – Plan de Implantación Entregables: • Plan de Implantación • Análisis y Diseño arquitectura • Plan de pruebas, para validar la puesta en servicio	*2 meses a partir del inicio de la ejecución*	
HITO_02	Instalación y Configuración de los equipos y licencias Entregables: • Documento técnico con la configuración realizada •	*2 meses después de la aceptación del HITO_01*	

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

HITO_03	Transferencia de conocimiento y documentación Entregables: • Plan de implantación actualizado • Diseño arquitectura actualizado • Documento técnico con la configuración realizada • Plan de pruebas ejecutado • Manual de operación y Monitorización	*2 meses después de la aceptación del HITO_02*	
…	…		

II.2. SERVICIOS DE SOPORTE DE LOS SUMINISTROS

Alcance

Gestionar el mantenimiento de la garantía requerida del fabricante.

Mantenimiento de adjudicatario en 24x7 con:

- Gestión de garantía (y extensión garantía)
  - Gestión de reemplazos (reemplazo avanzado de piezas averiadas)
  - Acceso al TAC del fabricante para resolución de casos
  - Acceso a las actualizaciones de las versiones de software de los equipos y acceso a parches que resuelvan fallos.
  - Acceso a datasheets y especificaciones del fabricante. Release notes.
  - El soporte deberá estar registrado en el fabricante a nombre del CSN.
  - El CSN podrá acceder a las actualizaciones del fabricante si así lo considera.
  - Atención a consultas del servicio
  - Actualizaciones de los dispositivos, que se harán “in situ” siempre que el CSN lo considere necesario.
- Disponibilidad de un service desk para reporte de incidencias o casos de soporte
  - Gestión y atención de incidencias
  - Gestión de reemplazos (vía garantía y/o stock)
  - Atención a consultas del servicio.
  - Acceso a portal web para la consulta de incidencias.
  - Gestión de inventario estándar.
- Mantenimiento evolutivo:
  - Suministro de información y recomendaciones ante consultas sobre nuevas actualizaciones
  - actualización del software y firmware de los cortafuegos a la última versión disponible, tanto versiones menores como mayores, al mes de su liberación y bajo

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

supervisión y aprobación del Responsable del Contrato, que en cualquier caso podrá decidir ampliar el plazo para efectuar dicha actualización. Esta actuación se hará "in situ" siempre que el CSN lo considere necesario.

- Mantenimiento Correctivo
  - Mantenimiento Primer nivel:
    - Contacto y coordinación con el fabricante para resolución de incidencias
    - Presencia "in situ" para reemplazo de piezas
  - Mantenimiento Segundo nivel: Diagnóstico y resolución de incidencias complejas.
  - Mantenimiento Tercer nivel
    - Apertura y seguimiento de casos específicos con el fabricante
    - Escalado y soporte con el fabricante

El soporte incluye, asimismo, una bolsa de 50 horas para integración con otras infraestructuras del CSN (NAC, VPN, FWs, etc) durante el plazo de garantía y soporte de este expediente.

Horario de servicio

El soporte deberá ser **24x7** en general para las incidencias según el ANS establecido en el punto II.2.2.

En caso de consultas o mantenimiento evolutivo el horario habitual establecido será de lunes a viernes en la franja horaria que disponga el CSN. Con carácter general, salvo que explícitamente se indique otra, se estima una jornada semanal de cuarenta horas partiendo de los supuestos siguientes:

- Jornada de prestación del servicio: 8 horas.
- Días: de lunes a viernes (no se contemplan festivos).

El horario estándar aplicará a casos de consulta y mantenimiento evolutivo.

Independientemente de vacaciones y otros permisos personales el contratista deberá garantizar la prestación del servicio, por lo que el recurso asignado a los casos de soporte deberá ser cubierto por un recurso de igual o superior cualificación y en las mismas condiciones de prestación del servicio.

II.2.1. DIMENSIONAMIENTO DEL SERVICIO

NO APLICA

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.

El tipo de soporte será en modalidad 24*7

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

En el marco de este servicio, se establecen los siguientes tiempos de respuesta y de resolución, con sus respectivos porcentajes de nivel de cumplimiento, como acuerdos de nivel de servicio mínimos para cada tipo de incidencia, según los niveles de gravedad que se establecen:

Nivel de gravedad	Impacto	Tiempo de respuesta	Nivel de cumplimiento	Tiempo de resolución	Nivel de cumplimiento
1	Incidencia grave: error o avería en el sistema con pérdida total o parcial del servicio.	15 minutos desde la notificación o detección	99 %	Menos de 4 horas	99 %
2	Degradación del servicio: error o avería en el sistema que no implica pérdidas de servicio pero sí su degradación, como, por ejemplo, la caída de un componente redundante.	30 minutos desde la notificación o detección	97%	Menos de 12 horas	97%
3	Peticiones de servicio por parte del CSN: - Eventos sin pérdida de servicio pero potencialmente peligrosos. - Eventos excepcionales, no previstos o singulares que, sin afectar a la prestación o a la calidad del servicio se puedan catalogar de anormales (por ejemplo, intentos de intrusión).	4 horas desde la notificación o detección	95%	Menos de 24 horas	95%
4	Sin impacto en el servicio: tareas programadas.	NBD		En el plazo acordado	

Cualquier problema, avería, encargo, petición o consulta se considerará una incidencia, con independencia que la misma haya sido abierta o informada por el CSN, abierta proactivamente por los servicios técnicos del adjudicatario, o puesta de manifiesto por los sistemas de monitorización del adjudicatario.

El adjudicatario deberá proveer al CSN de una herramienta, tipo Jira o similar, que permita registrar las incidencias o peticiones y hacer el seguimiento del cumplimiento de los acuerdos de nivel de servicio comprometidos.

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

Los trabajos de instalación avanzada serán realizados por técnicos convenientemente cualificados, mediante las certificaciones de máximo nivel por parte del fabricante, que muestre su capacidad para implantar la solución ofertada.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

Respecto al servicio de soporte, se precisa que lo dirija un ingeniero de Seguridad, con categoría de Consultor y una experiencia mínima de 5 años en puestos similares, con el máximo nivel de certificación del fabricante.

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

ANEXO III TRATAMIENTOS DE DATOS, FINALIDAD Y MEDIDAS

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

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

***NO APLICA

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

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

III.2. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

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

***NO APLICA

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

ANEXO IV ENTREGAS PARCIALES

***NO APLICA

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

ANEXO V 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 aplicación de actualizaciones de firmware y software, en los términos descritos en el PPT;
- Otras actuaciones preventivas encaminadas a evitar fallos del equipo, según lo indicado en el documento de invitación.

Horario de contacto: 24x7 para incidencias de nivel 1 o 2 según ANS

Acuerdos de nivel de servicio: los indicados en II.2.2

Id.	Nombre	Descripción del indicador	Valor
ANS_01	*Tiempo de respuesta*	*Tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo de sopoorte comunica que ha empezado a trabajar en su resolución.*	*X horas / días*
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.*	*X horas / días*
ANS_03	*Tiempo de resolución de incidencia grave*		*X horas / días*
ANS_04	*Tiempo de resolución de incidencia crítica*		*X horas / días*
…	…	…	…

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

ANEXO VI MODELO DE NOTIFICACIÓN DE SUBCONTRATACIÓN

D. ....., con DNI o documento equivalente en caso de extranjeros o. pasaporte nº....., en su propio nombre, o como representante legal de la empresa ....., adjudicataria del CONTRATO ESPECÍFICO Nº ..... del SISTEMA DINÁMICO PARA EL SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (SDA 24/2021; Expediente 2022/68), pongo en conocimiento del órgano de contratación, a los efectos del artículo 215.2.b) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), que, para la prestación indicada, se subcontrata con la/s siguiente/s entidad/es:

(Indicar:

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

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

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

- **Declaración responsable** de los subcontratistas de no hallarse incurso en prohibición de contratar, conforme el art. 71 de la LCSP.[10]
- **Certificación positiva** de la Agencia Estatal de Administración Tributaria de hallarse los subcontratistas al corriente en el cumplimiento de las obligaciones tributarias o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.
- **Certificación positiva** de la Tesorería General de la Seguridad Social de hallarse los subcontratistas al corriente de sus obligaciones con la Seguridad Social o, alternativamente, **autorización** al órgano de contratación para obtener de forma directa la acreditación de este extremo.

....., a ..... de ..... de .....

Firmado electrónicamente

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

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

Efectúa las siguientes **DECLARACIONES**

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

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

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

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

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

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

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

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

Acredita **la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT** (declaración censal 036 o 037[11] o documento equivalente de las Administraciones Forales) que incluye la actividad objeto del contrato basado conforme a lo previsto en el artículo 8 apartado 2 de la Orden HFP/1030/2021, de 29 de septiembre).

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

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

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

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

……., XX de ……. de 202X
Fdo. ……

Cargo: ……

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

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

En todos los contratos específicos financiados[12] por el presupuesto de la Unión Europea resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiables, estableciéndose las siguientes **obligaciones**:

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

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

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

2. PRINCIPIO DO NO SIGNIFICANT HARM ("DNSH")

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

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

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

4. AUSENCIA DE CONFLICTO DE INTERESES

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

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

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

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

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

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

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

7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

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

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

8. PROHIBICIÓN DE DOBLE FINANCIACIÓN

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

1. RÉGÍMEN JURÍDICO APLICABLE

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

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

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

El contrato se enmarca en el **Componente** xx. **Inversión** xx

(Incluir denominación del componente inversión)

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

Etiquetado verde	Etiquetado digital
Incluir %	*Incluir %*

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

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

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

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

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

3.- CLÁUSULA DE MODIFICACIÓN DE LOS CONTRATOS BASADOS/ESPECÍFICOS FINANCIADOS EN EL PRTR

Sin perjuicio de las causas de modificación previstas en el documento de invitación, en caso de estar financiado el presente contrato basado/específico con cargo al PRTR, podrá ser modificado, si la Autoridad Responsable del mecanismo ordena la adopción de medidas correctoras por haberse evidenciado deficiencias durante la ejecución del contrato que afectan a alguno de los objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020 que pueden causar un daño significativo al medioambiente.

4.- PENALIDADES POR EJECUCIÓN DEFECTUOSA O INCORRECTA EJECUCIÓN DE LOS CONTRATOS ESPECÍFICOS FINANCIADOS EN EL PRTR

(Marcar si procede y definir, en su caso, cuantías)

En caso de incumplimiento o cumplimiento defectuoso por el contratista de los compromisos adquiridos en base a las obligaciones establecidas en este documento de invitación en relación al PRTR, se podrán imponer al contratista las siguientes penalidades conforme a lo previsto en los artículos 192 a 195 de la LCSP:

( ) Por incumplimiento de las obligaciones establecidas para los productos en el etiquetado verde o etiquetado digital.

( ) Por falta de acreditación a requerimiento del responsable del contrato en el plazo de 10 días hábiles. *(Definir cuantía o % si se marca la penalidad)*

( ) Por incumplimiento. *(Definir % si se marca la penalidad)*

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

( ) Por incumplimiento de las obligaciones asociadas al DNSH del componente/inversión: *(Definir % si se marca la penalidad)*

( ) Otras penalidades

(Definir)

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

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

Por ello, en base a lo establecido en el artículo 7 de la Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia, en caso de que no existan datos de titularidad real en las bases de datos de la AEAT de **un participante en el procedimiento de contratación,** el órgano de contratación solicitará a éste la información de su titularidad real. Esta información deberá aportarse al órgano de contratación en el plazo de cinco días hábiles desde que se formule la solicitud de información. La falta de entrega de dicha información en el plazo señalado será motivo de **exclusión** del procedimiento.

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

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718

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

FIRMADO ELECTRÓNICAMENTE - 08/05/2024 10:27:03 CET - copia obtenida del original
Firmado por: Javier Lopez Orcajo
La autenticidad del documento puede ser comprobada en: https://www.csn.es/Sede20/verificarcsv/formulario?csv=465C5-66165-D6152-87718