

# INFORME DE CONTRATACIÓN

**N.º INFORME DE CONTRATACIÓN:** 925/2025

**Expediente:** 18174/2025

**Procedimiento:** Contrataciones



## PROCEDIMIENTOS ABIERTOS

### INFORME JUSTIFICATIVO DE NECESIDAD DE CONTRATACIÓN

Don Ruymán Belda Dieppa, coordinador de la Dirección de Servicios TIC e Instalaciones, en cumplimiento de la Ley 9/2017, de 8 de noviembre, de contratos del sector público **SOLICITA** la iniciación de un expediente de contratación cuyos datos se detallan a continuación:

**Código de Proyecto:** no aplica

**Administración de la que proviene el encargo:** no aplica

**Existe verificación:** no aplica

**Encomienda origen de la actuación:** no aplica

**Estado de la encomienda:** no aplica

**Finalización del plazo de ejecución de la encomienda:** no aplica

**Porcentaje de medios propios referidos a la encomienda:**

**Porcentaje de medios propios referidos a la encomienda:**

<b>más del 50%</b>		
<b>menos del 50%</b>	<b>%</b>	<b>porcentaje previsto <sup>(1)</sup></b>

**Con la nueva ley de contratos el importe de las prestaciones parciales que se puede contratar con terceros no excederá del 50% de la cuantía del encargo (artículo 32.7b)**

**Tipo de Contrato:** suministros

**Objeto del Contrato:** Suministro de cuatro dispositivos firewall, antivirus y MDR (seguridad gestionada) para renovar la plataforma de seguridad perimetral y protección de endpoints, así como los servicios de soporte experto que aseguren una adecuada gestión. La solución deberá incluir un firewall de nueva generación con protección avanzada contra amenazas y una solución de protección para endpoints que garantice seguridad ante malware, ransomware y ataques avanzados.

**Cofinanciación Europea:** NO

**Presupuesto:**

1. **El presupuesto base de licitación:** El presupuesto total asciende a 208.650,00 € (incluyendo el 7% de I.G.I.C):



2. **El valor estimado del contrato:** El presupuesto total sin impuestos indirectos asciende a 195.000,00 €:

El valor estimado del contrato se ha obtenido en base a los precios de mercado.

**Determinación de los costes directos e indirectos:**

En el concepto de valor estimado del contrato, se consideran incluidos los costes directos (ejecución material), e indirectos (gastos generales de estructura y beneficio industrial), que la empresa adjudicataria necesite para la realización del contrato de suministro propiamente dicho, y de acuerdo a las condiciones establecidas en los Pliegos.

Dichos costes dependen de los procesos de fabricación y suministro de cada licitador, por lo que no es posible prever un importe concreto. No obstante, y de acuerdo a la RECOMENDACIÓN 1/2021 DE 28 DE OCTUBRE, SOBRE GASTOS GENERALES Y BENEFICIO INDUSTRIAL EN LOS CONTRATOS DEL SECTOR PUBLICO CANARIO, publicado por la Junta Consultiva de Canarias, se estiman, a priori, los siguientes porcentajes e importes:

Gastos generales (17%)	26.951,22 €
Beneficio industrial (6%)	9.512,20 €
<b>Costes indirectos (23%)</b>	<b>36.463,41 €</b>

Costes directos	158.536,59 €
Costes indirectos (23%)	36.463,41 €
<b>Valor estimado del contrato</b>	<b>195.000,00 €</b>
I.G.I.C.(7%)	13.650,00 €
<b>Presupuesto base licitación</b>	<b>208.650,00 €</b>

**Plazo de ejecución:** Periodo de 4 meses desde la formalización del contrato

Duración de las licencias y servicios asociados: Las licencias de software, suscripciones de seguridad y servicios MDR incluidos en el presente contrato tendrán una duración de 36 meses contados desde la fecha de aceptación de la instalación, asegurando la continuidad del servicio y la protección durante todo el periodo de vigencia.

**Procedimiento de contratación:** Procedimiento abierto.

**Solvencia técnica o profesional:**

La solvencia técnica o profesional tendrá que acreditarse por alguno de los medios siguientes:



- a) Declaración responsable debidamente firmada por el licitador, indicando una relación de los principales suministros similares efectuados durante los tres últimos años, que incluya su importe, fechas y destinatario público o privado de los mismos. Esta declaración se entregará junto con la presentación de las ofertas.
- b) Indicación del personal técnico o unidades técnicas, integradas o no en la empresa, de los que se disponga para la ejecución del contrato.

### **Solvencia económica y financiera:**

La solvencia económica y financiera de los empresarios deberá acreditarse por alguno de los siguientes medios:

- a) Mediante el volumen anual de negocios, o bien volumen anual de negocios en el ámbito al que se refiera el contrato, referido al mejor ejercicio dentro de los tres últimos disponibles en función de las fechas de constitución o de inicio de actividades del empresario y de presentación de las ofertas por importe igual o superior al exigido en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato o, en su defecto, al establecido reglamentariamente.
- b) En los casos en los que resulte apropiado, justificante de la existencia de un seguro de responsabilidad civil por riesgos profesionales por importe igual o superior al exigido en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato o, en su defecto, al establecido reglamentariamente

La acreditación documental de la suficiencia de la solvencia económica y financiera del empresario se efectuará mediante la aportación de los certificados y documentos que para cada caso se determinen reglamentariamente, de entre los siguientes: certificación bancaria, póliza o certificado de seguro por riesgos profesionales, cuentas anuales y declaración del empresario indicando el volumen de negocios global de la empresa.

En virtud de lo dispuesto en el artículo 86.1 de la LCSP, cuando por una razón válida, el operador económico no esté en condiciones de presentar las referencias solicitadas por el órgano de contratación, se le autorizará a acreditar su solvencia económica y financiera por medio de cualquier otro documento que el poder adjudicador considere apropiado.

### **Concreción de las condiciones de solvencia (Artículo 76 LCSP).**

Con el fin de garantizar la adecuada ejecución del contrato, los licitadores deberán comprometerse a adscribir, de forma efectiva y exclusiva, los siguientes medios personales durante toda la duración del mismo:

- 1 Responsable Técnico de Ciberseguridad, con al menos 3 años de experiencia acreditada en implantación, configuración y gestión de soluciones de seguridad perimetral y protección de endpoints.



- 1 Técnico certificado en la tecnología ofertada, disponible presencialmente para las fases de implantación, seguimiento e intervención en caso de incidencias críticas, en cada una de las islas donde se ubiquen los equipos.
- Personal adicional necesario para la correcta ejecución del servicio, incluyendo consultoría, soporte, seguimiento e integración con soluciones existentes, debidamente cualificado.

El compromiso de adscripción de medios personales deberá presentarse en el archivo electrónico único junto con la proposición y la documentación administrativa, mediante una CARTA DE COMPROMISO firmada por el licitador.

El incumplimiento del compromiso de adscripción de dichos medios a la ejecución del contrato será considerado causa de resolución contractual, conforme al artículo 211 de la LCSP.

### Justificación de la exigencia de medios personales:

La necesidad de estos perfiles técnicos se justifica por la complejidad y criticidad de la infraestructura de seguridad, que requiere personal cualificado para garantizar la correcta implantación, configuración y mantenimiento de la solución durante toda la vigencia del contrato.

### Criterios de adjudicación

De acuerdo con el artículo 145 de la LCSP, se establecen los siguientes criterios para la adjudicación del contrato, ponderados sobre un total de **100 puntos**:

#### **1. Criterios evaluables mediante cifras y fórmulas (máximo 100 puntos)**

##### **1A. Criterios cuantitativos (65 puntos - 65%)**

##### **1.1. Mejora en la oferta económica (máximo 65 puntos - 65%)**

- La mayor baja económica se valorará con **65 puntos**.
- Las ofertas sin baja recibirán **0 puntos**.
- Para el resto de ofertas, la puntuación se calculará mediante la siguiente fórmula de interpolación lineal:

$$P = \frac{65 \times (Bo - B)}{(Bo - Bmax)}$$

Donde:

- **P**: Puntuación obtenida.
- **Bo**: Oferta sin baja (valor estimado del contrato).
- **B**: Presupuesto ofertado.
- **Bmax**: Oferta con la mayor baja económica.
- 

**Importante:** Se deberá respetar el precio máximo de cada producto; si se supera en algún producto, **no se valorará la oferta**.

### **Documentación requerida para su evaluación:**

La propuesta económica deberá incluir de forma detallada:



- **Desglose de precios unitarios por cada componente ofertado:** licencias, hardware y servicios.
- **Importe total de la oferta económica**, que en ningún caso podrá superar los precios máximos establecidos en este documento.

### Justificación:

Este criterio permite evaluar objetivamente la eficiencia económica de las ofertas, incentivando propuestas competitivas que optimicen el gasto público sin menoscabar la calidad de los servicios. La puntuación se otorga mediante una **fórmula de interpolación lineal**, que distribuye los 65 puntos en función de la baja económica ofrecida con respecto al valor estimado del contrato.

- Esta fórmula garantiza una **proporcionalidad transparente**, premiando las ofertas más ventajosas económicamente, siempre y cuando no superen los precios máximos establecidos por componente.
- Con ello se asegura el **cumplimiento del principio de economía** en la contratación pública, sin comprometer la viabilidad técnica de la solución ofertada.

### Justificación legal:

Este criterio se ajusta plenamente a lo previsto en el artículo 145.2 a) de la LCSP, al tratarse de un criterio evaluable de forma automática mediante fórmulas matemáticas, que **no requiere juicio de valor** y **favorece la objetividad y comparabilidad directa** entre ofertas.

## 1B. Criterios cualitativos (máximo 35 puntos - 35%)

### 1.1 Calidad técnica de la solución propuesta (hasta 20 puntos - 20%)

Se valorará la calidad y solidez de la propuesta técnica en función del nivel de cumplimiento, escalabilidad y alineación con los requisitos avanzados. Se evaluará positivamente el valor añadido respecto a los mínimos exigidos, así como la adecuación de la solución a los siguientes aspectos clave:

- **Capacidad técnica y rendimiento del firewall (4 puntos):**  
Firewall con rendimiento claramente superior al mínimo exigido ( $\geq 40$  Gbps IMIX,  $\geq 10$  Gbps IPS,  $\geq 5$  M sesiones activas).
  - En caso de no cumplir estas capacidades mínimas mejoradas, se asignará **0 puntos**.
- **Integración nativa entre NGFW y EDR/XDR (3 puntos):**  
Evaluación del grado de integración entre las capas de seguridad perimetral y de endpoints.
  - Si no se justifica o no se aporta dicha integración, se asignará **0 puntos**.



- **Consola de administración centralizada y visibilidad global (3 puntos):**

Capacidad para administrar de forma unificada endpoints, red y servicios MDR, con visibilidad total.

Se valorará especialmente la visibilidad extendida que abarque red, endpoints, correo, nube y servicios MDR, superando el requisito mínimo del Pliego Técnico.

- Si la consola no permite esta gestión unificada, la puntuación será **0 puntos**.

- **Funcionalidades avanzadas (3 puntos):**

Inclusión de servicios como NDR, WAF, ZTNA, filtrado DNS y sandboxing.

- Si no se incluyen estas funcionalidades, la puntuación será **0 puntos**.

- **Arquitectura modular, ampliable y con soporte a cloud híbrida (2 puntos):**

Flexibilidad para adaptarse a distintos entornos y fabricantes, con arquitectura escalable.

- La ausencia de estas características implicará **0 puntos**.

- **Integración con SIEM, herramientas de red y plataformas de productividad (2 puntos):**

Capacidad para integrarse con entornos como Microsoft 365, Google Workspace, SIEM y otras herramientas externas.

- En caso de no aportar esta interoperabilidad, se asignará **0 puntos**.

- **Adecuación a la normativa ENS en categoría ALTA (3 puntos):**

Se valorará el grado de cumplimiento con los requisitos del Esquema Nacional de Seguridad (ENS), nivel ALTO, por parte de los productos ofertados (por ejemplo, firewall o EDR/XDR).

En caso de que algún componente no disponga aún de la certificación definitiva, se aceptará estar en proceso de certificación ENS ALTA, debidamente acreditado mediante documentación oficial del fabricante o del Centro Criptológico Nacional (CCN).

En ausencia de cumplimiento o justificación documental, se otorgarán 0 puntos.

La propuesta deberá incluir:

- Descripción detallada de la arquitectura de seguridad (firewall, EDR/XDR, MDR).
- Características técnicas de cada componente con fichas técnicas oficiales.
- Integración de consola y compatibilidad con soluciones de terceros.
- Funcionalidades específicas: alta disponibilidad, sandboxing, WAF, NDR, DNS, etc.
- Plan de escalabilidad y actualización.





- Detalles sobre instalación, configuración, puesta en marcha y formación ofertada.

### Justificación:

Este criterio valora el grado de **adecuación técnica, innovación, escalabilidad y valor añadido** de la solución propuesta. Se desglosa en subcriterios objetivos, centrados en:

- **Capacidad técnica del firewall** y sus funcionalidades avanzadas (IPS, IMIX, sesiones).
- **Nivel de integración entre capas de seguridad** (NGFW + EDR/XDR).
- **Consola de administración centralizada** para una gestión unificada.
- **Funcionalidades avanzadas** como NDR, WAF, sandboxing, ZTNA, etc.
- **Modularidad y compatibilidad con cloud híbrido.**
- **Integración con plataformas externas (SIEM, M365, etc.).**
- **Cumplimiento del ENS en categoría ALTA.**

Este criterio, evaluado mediante juicio de valor técnico con base documental, permite seleccionar **la solución más sólida, segura y alineada con los objetivos estratégicos del contrato.**

### Justificación legal:

Este criterio cumple con el artículo 145.4 y 145.5 de la LCSP, ya que:

- Está **directamente vinculado al objeto del contrato.**
- Permite valorar aspectos técnicos que afectan a la **eficiencia, calidad y sostenibilidad de la solución.**
- Es **proporcionado**, ya que representa un 20% del total de la puntuación.
- Está desglosado en **subcriterios claros y objetivos**, con un reparto de puntos justificado y equilibrado.

## 1.2 Certificaciones técnicas y de seguridad del fabricante (hasta 10 puntos - 10%)

Se valorará la presentación de certificaciones oficiales en vigor. Se otorgará:

- **Hasta 10 puntos por certificaciones del producto/solución:**  
Se evaluará positivamente que los productos ofertados (firewall, EDR/XDR, etc.) cumplan con estándares internacionales reconocidos en materia de seguridad y calidad.  
Las certificaciones admitidas, entre otras, incluyen:
  - Common Criteria EAL4+
  - FIPS 140-2 o FIPS 140-3
  - Certificación STIC emitida por el CCN para cumplimiento del ENS en categoría ALTA, cuando sea aplicable al productoEn el caso de soluciones que se encuentren en proceso de certificación ENS ALTA, se admitirá la aportación de documentación oficial que acredite dicho proceso, valorándose positivamente.

- **Criterios de puntuación orientativa:**





- 1 certificación relevante: 2,5 puntos
- 2 certificaciones relevantes: 5 puntos
- 3 certificaciones: 7,5 puntos
- 4 o más certificaciones: 10 puntos

**Documentación requerida para su acreditación:**

Deberá aportarse copia válida y en vigor de las siguientes certificaciones:

- Certificaciones técnicas del producto o solución propuesta (por ejemplo, Common Criteria, FIPS, STIC del CCN).

**Justificación:**

Este criterio valora el **nivel de fiabilidad, calidad y cumplimiento normativo** de la solución ofertada, mediante certificaciones reconocidas como:

- Common Criteria EAL4+
- FIPS 140-2 / 140-3
- STIC del CCN para cumplimiento del ENS en categoría ALTA

Las certificaciones aportadas aseguran que el producto ha superado **pruebas rigurosas de seguridad y calidad**, y está **reconocido por organismos oficiales o independientes**, reforzando la confianza en la solución ofertada.

**Justificación legal:**

Se trata de un criterio cualitativo basado en **documentación objetiva**, conforme al artículo 145.4 de la LCSP, directamente vinculado al objeto del contrato. Favorece soluciones **certificadas y contrastadas** a nivel internacional, reduciendo el riesgo tecnológico y reforzando la seguridad.

**1.3 Bolsa de horas de desarrollo y formación adicional (hasta 5 puntos - 5%)**

Se valorará la oferta de una **bolsa adicional de horas gratuitas** por parte del licitador, destinada a cubrir acciones de valor añadido una vez implantada la solución. Esta bolsa podrá emplearse en:

- Formación práctica adicional al personal de GESPLAN
- Tareas de mejora continua o evolución de la solución
- Adaptaciones, desarrollos menores, ajustes o informes personalizados

**Criterios de puntuación:**

- **Más de 30 horas** ofrecidas: **5 puntos**
- **Entre 10 y 30 horas**: **3 puntos**
- **Menos de 10 horas o no aportadas**: **0 puntos**

**Documentación requerida:**

Se deberá aportar una **carta de compromiso** firmada por el licitador que incluya:

- Número total de horas ofertadas de manera gratuita



- Alcance y condiciones de uso de dichas horas (por ejemplo, soporte post-implantación, formación adicional, personalización de informes o políticas, etc.)

### Justificación:

Este criterio premia el **compromiso proactivo del licitador** en el éxito de la implantación y evolución de la solución, valorando la oferta de horas gratuitas para:

- Formación adicional del personal.
- Ajustes, mejoras o informes personalizados tras la puesta en marcha.

Este tipo de valor añadido contribuye a una mejor **transferencia de conocimiento, mejora continua y adaptación a necesidades reales** una vez finalizada la entrega inicial.

### Justificación legal:

Este criterio cumple lo establecido en el artículo 145.5 LCSP, al:

- Estar vinculado al objeto del contrato (servicios de soporte y formación).
- Promover una mayor **eficiencia y continuidad en la implantación**.
- Valorar un aspecto relevante que **no se refleja en el precio ni en las especificaciones mínimas**.

## 2. Criterios de desempate

De acuerdo con el artículo 147.2 de la LCSP, en caso de empate tras la aplicación de los criterios anteriores, se resolverá aplicando, por orden, los siguientes criterios:

- a) Mayor porcentaje de trabajadores con discapacidad o en situación de exclusión social en la plantilla de la empresa licitadora, priorizando en caso de igualdad el mayor número de trabajadores fijos con discapacidad o en inclusión.
- b) Menor porcentaje de contratos temporales en la plantilla de la empresa licitadora.
- c) Mayor porcentaje de mujeres empleadas en la plantilla de la empresa licitadora.
- d) Sorteo, en caso de que los criterios anteriores no resuelvan el empate.

**Pliego de Prescripciones Técnicas:** Se adjunta.

**Código CPV del Reglamento Europeo por el que se aprueba el vocabulario común de contratos:**

30237000-9: Licencias de firewall.

48820000-2: Firewall interno

48900000-7: Firewall interno

72500000: Servicios informáticos (para servicios relacionados con firewalls).

48760000: Paquetes de software de protección antivirus



32420000: Equipo de red (si el firewall es un dispositivo de red).

50324100: Servicios de mantenimiento de sistemas (si el contrato incluye servicios de mantenimiento del firewall).

### **Clasificación:**

Para ser adjudicatario del presente contrato no es preciso estar en posesión de clasificación empresarial alguna, sin perjuicio de acreditar la correspondiente solvencia económica, financiera y técnica o profesional por los medios establecidos en el presente Informe justificativo.

### **Ofertas anormalmente bajas:**

Se considerarán, en principio, anormalmente bajas las ofertas que se encuentren en los siguientes supuestos:

- Un licitador: Se considerará, en principio, anormalmente baja la oferta que sea inferior al valor estimado de contrato en más de un 25%.
- Dos licitadores: Se considerará, en principio, anormalmente baja la oferta que sea inferior en más de un 20% a la otra oferta.
- Tres o más licitadores: Se considerará, en principio, anormalmente baja la oferta que sea inferior en más de un 10% a la media aritmética de las ofertas presentadas.

En los criterios no económicos la puntuación está establecida de manera que, o los tiene, o no, no existe puntuación intermedia, con lo que las empresas participantes solo tienen la opción de acreditar y si no, no puntúan, es decir, no hay posibilidad de ofertas anormalmente bajas.

**Servicio del anexo IV de la LCSP:** No

**Servicio del anexo VI de la LCSP:** No.

**Prestación de carácter intelectual:** No.

**Garantía:** En virtud de lo dispuesto en el artículo 114 de la LCSP no se exige.

### **Documentación a incluir en el archivo electrónico:**

Los licitadores deberán presentar, en el archivo electrónico único, la siguiente documentación, con el fin de garantizar el cumplimiento de los requisitos del pliego y permitir una correcta valoración de las ofertas:

#### **1. Declaración responsable**

Manifestando el cumplimiento de las obligaciones establecidas en el Pliego



de Prescripciones Técnicas, así como el respeto a la normativa vigente en materia de:

- o Seguridad de la información (ENS, NIS 2)
- o Protección de datos personales (RGPD)
- o Contratación pública (LCSP)

2. **Documentación acreditativa de la cualificación y experiencia de los medios personales adscritos al contrato**

**La decisión de no dividir el objeto del contrato en lotes.** (art. 116.4 g) LCSP).

El objeto del contrato consiste en el suministro, implantación, integración y mantenimiento de una **plataforma unificada de seguridad perimetral y protección avanzada de endpoints**, lo cual constituye un **proyecto integral** que debe garantizar la interoperabilidad, la continuidad del servicio y la eficacia de las medidas de ciberseguridad desplegadas.

Dado que los distintos componentes de la solución (firewall de nueva generación, EDR/XDR, consola de administración, servicio MDR 24/7, protección de correo y servidores, etc.) **forman parte de un ecosistema técnico interdependiente**, la división en lotes podría provocar problemas de integración, incompatibilidades entre fabricantes, duplicidad de agentes, y pérdida de visibilidad y capacidad de respuesta coordinada ante amenazas.

Además, la contratación de un único adjudicatario:

- Asegura una **gestión centralizada** de políticas y eventos desde una consola única.
- Facilita la **intervención eficaz del servicio MDR**, que actúa sobre todos los dispositivos integrados.
- Permite una **planificación, formación y soporte homogéneos**, reduciendo los riesgos operativos.
- Evita **solapamientos o lagunas de responsabilidad** entre distintos proveedores.

Por tanto, y en virtud de lo dispuesto en el artículo 116.4 g) de la LCSP, se considera justificada la **no división del contrato en lotes**, al tratarse de una solución técnica integrada cuyo fraccionamiento podría afectar negativamente a la seguridad, interoperabilidad y eficiencia del servicio prestado.

**Subcontratación:** Se permite la subcontratación según lo establecido en el artículo 215 de la LCSP, debiendo el licitador cumplir los requisitos exigidos en dicho artículo.

**En cuanto a la normativa en materia de Protección de Datos:**

Durante el desarrollo del contrato, el adjudicatario deberá garantizar el cumplimiento estricto de la normativa vigente en materia de protección de datos personales, en especial el **Reglamento (UE) 2016/679, General de Protección de Datos (RGPD)**, y la **Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**.

Dado que la solución propuesta incluye herramientas que recopilan, analizan y tratan información relativa a usuarios, dispositivos y eventos de seguridad en la



red corporativa (tales como soluciones de EDR/XDR, firewall, MDR y consolas de gestión centralizada), **se producirá tratamiento de datos personales** en el marco de la ejecución del contrato. Por tanto, el adjudicatario deberá:

- Garantizar la **implantación de medidas técnicas y organizativas adecuadas**, que aseguren la **confidencialidad, integridad y disponibilidad** de los datos tratados por los sistemas.
- Configurar e implantar la solución conforme a los principios de **“Privacidad desde el Diseño y por Defecto”**, minimizando la recogida de datos y estableciendo controles granulares de acceso, trazabilidad y auditoría.
- Asegurar que la solución **sea compatible con las políticas de privacidad** de la entidad contratante y permita:
  - o La configuración de permisos por rol.
  - o El acceso controlado a los datos.
  - o La **monitorización segura y transparente de eventos**.
- Garantizar que **los datos personales no serán utilizados para finalidades ajenas al contrato**, ni serán cedidos a terceros sin consentimiento expreso o sin habilitación legal o contractual.
- En caso de que el adjudicatario tenga acceso a sistemas, usuarios o dispositivos que contengan datos personales, deberá suscribir un **acuerdo de confidencialidad** y, en su caso, un **contrato de encargo de tratamiento**, de conformidad con el artículo 28 del RGPD.

La entidad podrá solicitar evidencia documental del cumplimiento de estas obligaciones, así como informes de medidas técnicas implantadas, esquemas de privacidad aplicados y certificados de cumplimiento normativo por parte del adjudicatario.

**La necesidad de iniciarse el correspondiente expediente de contratación se basa en los siguientes extremos:**

La presente contratación responde a la necesidad estratégica de **reforzar las capacidades de ciberseguridad de la entidad**, garantizando la continuidad operativa, la protección frente a amenazas avanzadas y la adecuación a las nuevas exigencias normativas y tecnológicas.

En un entorno cada vez más digitalizado, donde la información constituye uno de los activos más valiosos, **la seguridad perimetral y la protección de endpoints** se convierten en elementos clave para asegurar la confidencialidad, integridad y disponibilidad de los sistemas corporativos. La evolución de las amenazas (malware, ransomware, ataques dirigidos, APTs) exige dotarse de herramientas modernas, integradas y coordinadas que permitan detectar, contener y responder eficazmente ante incidentes.

La infraestructura actualmente en uso presenta limitaciones tanto funcionales como de rendimiento, y no responde a las necesidades actuales ni a las exigencias futuras en materia de:

- Visibilidad unificada de red y endpoints.
- Capacidad de respuesta automatizada y coordinada (XDR/MDR).



- Cumplimiento de normativas de seguridad como el **ENS**, la **Directiva NIS 2**, el **RGPD**, o los **requisitos del CCN-CERT**.

Por tanto, se hace imprescindible acometer la **renovación integral de la plataforma de seguridad**, incorporando:

- Dispositivos **firewall de nueva generación (NGFW)**.
- Soluciones avanzadas de **detección y respuesta (EDR/XDR)**.
- **Servicio MDR 24x7** para la monitorización continua y la respuesta ante incidentes.
- Consola centralizada para la gestión global de políticas de seguridad y visibilidad de amenazas.
- Servicios de formación, soporte experto y despliegue con presencia local.

Esta actuación está plenamente alineada con la **estrategia de digitalización, modernización y resiliencia** de la organización, y tiene como objetivo establecer un entorno tecnológico **más robusto, eficiente y seguro**, que permita a la entidad afrontar con garantías los retos actuales y futuros.

En las Palmas de Gran Canaria, a fecha de la firma electrónica





## **Pliego de Prescripciones Técnicas para la adquisición de cuatro dispositivos firewall, antivirus y MDR**

### **1. OBJETO.**

El objeto del presente pliego tiene por objeto describir las características técnicas del suministro de cuatro dispositivos firewall, antivirus y MDR (seguridad gestionada) para renovar la plataforma de seguridad perimetral y protección de endpoints, así como de los servicios de soporte experto que aseguren una adecuada gestión. La solución deberá incluir un firewall de nueva generación con protección avanzada contra amenazas y una solución de protección para endpoints que garantice seguridad ante malware, ransomware y ataques avanzados.

### **2. ASPECTOS TÉCNICOS Y SERVICIOS REQUERIDOS**

El equipamiento y servicios suministrados deberán cumplir con los siguientes requisitos generales:

- Las soluciones propuestas deberán ofrecer capacidades y rendimiento superiores al equipamiento actualmente en uso por la entidad, sin suponer en ningún caso un retroceso funcional o tecnológico.
- Las soluciones propuestas deberán pertenecer a fabricantes con reconocimiento internacional y con presencia en el mercado nacional.
- La propuesta deberá incluir una solución de protección avanzada para endpoints (EDR/XDR), capaz de hacer frente a malware, ransomware y amenazas persistentes avanzadas.
- Se valorará positivamente que la solución EDR/XDR cuente con un servicio MDR del mismo proveedor, o bien que sea integrable con servicios MDR de terceros.
- Se deberá incluir un firewall de nueva generación (NGFW) con capacidad para gestionar al menos 900 usuarios simultáneos, que permita integración o interoperabilidad con soluciones EDR/XDR para permitir acciones de respuesta coordinadas.
- La solución deberá contar con consola de administración centralizada con visibilidad sobre las políticas de seguridad, eventos de red y endpoints.
- El adjudicatario deberá proporcionar soporte técnico y formación suficiente al personal interno designado por la entidad.
- El personal encargado de la instalación, configuración y puesta en funcionamiento deberá contar con experiencia acreditada en





soluciones de seguridad similares y aportar certificaciones vigentes del fabricante o fabricantes propuestos, o equivalente.

### **3. CARACTERÍSTICAS Y REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL EQUIPAMIENTO FIREWALL**

#### **3.1 Reconocimientos de Terceros**

Para garantizar la fiabilidad y madurez de la solución, se requerirá que el firewall y/o su sistema operativo cumpla, al menos, con alguno de los siguientes estándares o certificaciones internacionales reconocidas en el sector de la ciberseguridad:

- Cumplimiento del Esquema Nacional de Seguridad en categoría ALTA o equivalente (p. ej., productos listados en el catálogo STIC 105 del CCN).
- Certificación de seguridad Common Criteria EAL4+ o superior (ISO/IEC 15408).
- Certificaciones adicionales de seguridad reconocidas: FIPS 140-2/3, IPv6 Ready, CE, FCC u otras equivalentes según normativa del país de origen.

#### **3.2 Arquitectura**

- La arquitectura del equipo debe estar basada en sistemas de procesamiento multiproceso (multicore), con separación lógica entre el plano de datos y el de control.
- Se valorará el uso de unidades especializadas para procesamiento de red (NPUs u otras) que optimicen el rendimiento y reduzcan la latencia.

#### **3.3 Especificaciones Técnicas Mínimas del Firewall**

##### **1. Formato y entorno**

- Diseño en formato rack 19”.
- Fuente de alimentación redundante o posibilidad de añadirla.
- Compatibilidad con entornos con PoE (opcional).

##### **2. Rendimiento mínimo requerido**

- Rendimiento sostenido del firewall  $\geq 40$  Gbps en tráfico mixto (IMIX).
- Rendimiento de IPS  $\geq 10$  Gbps.
- VPN IPsec  $\geq 10$  Gbps.
- Latencia máxima permitida en pruebas UDP de 64 bytes  $\leq 10$   $\mu$ s.
- Capacidad de conexiones simultáneas:  $\geq 5$  millones.



- Conexiones por segundo:  $\geq 100.000$ .

### 3. Interfaces mínimas

- Al menos 8 puertos GE RJ45, y al menos 2 puertos de fibra (SFP o SFP+).
- Al menos 1 puerto de administración dedicado (RJ45, consola o USB).
- Posibilidad de ampliación modular con interfaces adicionales.

### 4. Almacenamiento

- Capacidad de almacenamiento local no volátil para logs y cuarentena: mínimo 240 GB SSD.

### 5. Compatibilidad con virtualización y nube

- Soporte para entornos virtuales (VMware, Hyper-V, KVM u otros).
- Integración con plataformas en la nube pública (Azure, AWS u otras).

## 3.4 FUNCIONALIDADES MÍNIMAS REQUERIDAS

### 3.4.1. Alta Disponibilidad

- La solución deberá permitir configuración en alta disponibilidad (HA) en modos activo-activo o activo-pasivo.
- Se deberá garantizar la continuidad del servicio mediante redundancia de componentes críticos (fuentes de alimentación, interfaces, etc.) y de sesiones, incluyendo sesiones IPsec e IKE.
- El sistema deberá asegurar una disponibilidad mínima del 99,9%.

### 3.4.2. Autenticación

- Integración con servicios de directorio como Active Directory local y Azure AD.
- Soporte para autenticación única (Single Sign-On) basada en credenciales de dominio.
- Identificación de usuarios mediante agentes de seguridad instalados en los endpoints o mediante mecanismos equivalentes.
- Soporte para múltiples métodos de autenticación (AD, LDAP, RADIUS, multifactor, etc.).

### 3.4.3. Administración



- Plataforma de gestión basada en la nube o en local, con roles de administración configurables.
- Gestión centralizada de políticas, registros y alertas de seguridad.
- Soporte para copias de seguridad automáticas de configuración y logs.
- Integración con herramientas de monitorización mediante SNMPv3 o protocolos equivalentes.

#### **3.4.4. Funcionalidades del Firewall**

- Funcionalidad de firewall de nueva generación con capacidad de inspección profunda de paquetes (DPI).
- Sistema de detección y prevención de intrusiones (IDS/IPS), con posibilidad de definir reglas personalizadas y categorización de amenazas.
- Soporte para tecnologías SD-WAN, enrutamiento por políticas, balanceo de carga y VPN avanzadas.
- Capacidad de inspección de tráfico cifrado SSL/TLS, incluyendo soporte para TLS 1.3.
- Mecanismos de protección contra ataques DoS/DDoS y detección de tráfico malicioso en tiempo real.

#### **3.4.5. Acceso Remoto**

- Soporte para VPN IPsec y SSL, con capacidad para portal HTML5 sin cliente.
- Compatibilidad con dispositivos Zero-touch y despliegues remotos.
- Integración con soluciones ZTNA (Zero Trust Network Access) o equivalente.

#### **3.4.6. Control de Aplicaciones**

- Identificación, categorización y control del tráfico por aplicación, usuario o grupo.
- Capacidad para definir políticas de uso de ancho de banda y restricciones basadas en comportamiento.
- Integración con servicios de análisis del comportamiento en red o soluciones CASB.

#### **3.4.7. Filtrado Web**

- Filtro web basado en reputación y categorías, con análisis de contenido en tiempo real.
- Inspección de tráfico HTTPS con capacidad de filtrado y descifrado seguro.



- Posibilidad de aplicar políticas por usuario, grupo o dispositivo mediante integración con directorio.

#### **3.4.8. Calidad de Servicio (QoS)**

- Definición de reglas de priorización de tráfico por aplicación, dirección, usuario o servicio.
- Soporte para programación de políticas de tráfico y gestión dinámica del ancho de banda.

#### **3.4.9. Auto-remediación**

- Capacidad para aislar automáticamente dispositivos comprometidos.
- Integración con soluciones EDR/XDR o equivalentes para respuesta coordinada basada en eventos de seguridad.

#### **3.4.10. Informes y Registro de Eventos**

- Generación de informes automáticos y personalizables.
- Monitorización en tiempo real y almacenamiento local o en la nube de logs.
- Posibilidad de integración con soluciones SIEM mediante estándares abiertos (Syslog, CEF, etc.).

#### **3.4.11. Protección de Correo Electrónico**

- Filtro de correo con detección de amenazas, análisis de comportamiento y sandboxing.
- Soporte para análisis de adjuntos y enlaces en la nube, con capacidad de detección proactiva.

#### **3.4.12. Controladora WiFi**

- Capacidad para gestionar puntos de acceso WiFi, con soporte para modos mesh y control centralizado de SSID y políticas.

#### **3.4.13. Análisis Avanzado (Sandboxing)**

- Integración con sistemas de análisis en la nube para estudio del comportamiento de archivos sospechosos.
- Análisis a nivel de red y endpoint.

#### **3.4.14. Plataforma de Gestión Centralizada**



- Consola unificada para la gestión de firewall, endpoints y servicios de seguridad, ya sea nativa o mediante integración certificada.
- Soporte para almacenamiento centralizado de logs, configuración basada en plantillas y gestión basada en roles.

#### **3.4.15. Protección de Endpoints**

- Integración con soluciones EDR/XDR con capacidades de análisis y respuesta ante amenazas.
- Detección de amenazas sin necesidad de múltiples agentes.
- Capacidad de aislamiento de dispositivos, análisis de comportamiento y respuesta ante ransomware, APTs y amenazas de día cero.

#### **3.4.16. Protección DNS**

- Filtrado DNS por categorías configurables (mínimo 50).
- Detección de amenazas en consultas DNS con capacidad de respuesta en tiempo real.

#### **3.4.17. Detección y Respuesta en Red (NDR)**

- Incorporación o integración con soluciones NDR que permitan análisis de tráfico interno, detección de amenazas laterales y visualización de relaciones entre eventos.

#### **3.4.18. Gestión de IoCs**

- Posibilidad de importar indicadores de compromiso (IoCs) desde fuentes externas.
- Integración con endpoints para la correlación de eventos e identificación de vectores de ataque.

#### **3.4.19. Protección de Aplicaciones Web (WAF)**

- Funcionalidad de WAF con capacidad de proteger contra amenazas comunes (OWASP Top 10).
- Funcionalidades como form hardening, geo-blocking, escaneo de contenido, control de cookies y bloqueo de clientes maliciosos.
- Soporte para creación de formularios de autenticación personalizados, control de sesiones, límites de tiempo y análisis de tráfico HTTP/S.



Nota: Todas las funcionalidades deberán estar debidamente documentadas por el licitador e implementadas en soluciones con soporte técnico activo y ciclo de vida garantizado por el fabricante.

## 4. Características de la solución de Protección (EPP)

Este apartado detalla los **requisitos mínimos imprescindibles** que deben cumplir las soluciones propuestas para ser consideradas. Solo se valorarán las propuestas que cumplan todos los requisitos obligatorios.

### 4.1. Reconocimientos de terceros

- La solución deberá haber sido reconocida como líder en informes de análisis de mercado de los últimos años por consultoras de referencia internacional en ciberseguridad.
- Deberá cumplir con las recomendaciones de organismos nacionales de seguridad informática (por ejemplo, guías técnicas de buenas prácticas).
- Contar con evaluaciones comparativas independientes, públicas y recientes, realizadas por laboratorios de pruebas reconocidos del sector.

### 4.2. Consola de Administración

#### Requisitos obligatorios:

- La solución debe contar con una **consola unificada** para gestionar todas las funcionalidades del sistema, incluyendo la protección de endpoints, funciones de detección y respuesta (XDR/MDR), cifrado y acceso remoto seguro.
- Consola basada en la nube, alojada en centros de datos dentro de la UE o EE.UU., con posibilidad de elegir entre varias regiones disponibles.
- Debe permitir **una gestión basada en agentes modulares** que unifiquen todas las funcionalidades en una única instalación en el dispositivo.
- Autenticación multifactor con al menos tres métodos distintos.
- Posibilidad de federación con sistemas de identidad corporativos.
- Capacidad para crear **suborganizaciones** con distintos niveles de visibilidad y control administrativo.



- Gestión por roles, con perfiles predefinidos y opción de personalizar permisos granulares.

### **Políticas y operativa:**

- Aplicación de políticas por dispositivo o usuario, con sincronización con servicios de directorio empresarial.
- Registro de auditoría completo sobre acceso y cambios en la configuración.
- Actualizaciones programables, diferenciadas por tipo de versión (estable, pre-lanzamiento, extendida).
- Soporte para operaciones automatizadas como escaneos y actualizaciones sin intervención del usuario.
- Sistema de pruebas de políticas y actualizaciones mediante grupos piloto.
- Entrega de políticas y actualizaciones independientemente de la ubicación de los equipos.
- Capacidad para utilizar caches de actualización o relays internos para optimizar el uso de ancho de banda.
- Integración mediante API abierta con plataformas de análisis y eventos de seguridad (SIEM).

### **Visibilidad y corrección proactiva:**

- Debe mostrar el estado de salud de los dispositivos respecto a protección activa, configuración insegura, exclusiones no recomendadas, etc.
- Acciones correctivas disponibles desde la misma consola.

### **Opciones adicionales:**

- Gestión diferenciada del ancho de banda de actualización.
- Políticas específicas para clientes y servidores.
- Jerarquía de políticas con aplicación condicional.
- Protección contra manipulaciones y desinstalación mediante credenciales administradas.
- Modularidad y escalabilidad del sistema.
- Gestión de tamaño de logs para funciones avanzadas como XDR.





#### **4.2.2. Despliegue y sincronización con terceros**

- Posibilidad de despliegue mediante imágenes, GPO, MECM, instalador personalizable, correo o soluciones MDM.
- Integración con servicios de directorio locales y en la nube, tanto mediante agentes como nativamente en caso de directorios cloud.
- Integración opcional con plataformas cloud como Microsoft 365 o Google Workspace para una visión ampliada de seguridad.

### **4.3. Políticas Generales**

#### **4.3.1. Gestión del Firewall local:**

- Capacidad para monitorizar o gestionar perfiles de red del firewall del sistema operativo.

#### **4.3.2. Actualizaciones de software:**

- Políticas granuladas de actualización para distintos grupos de equipos.

#### **4.3.3. Prevención de fuga de información:**

- Creación de reglas por contenido, tipo de archivo o canal de comunicación, incluyendo múltiples medios.

#### **4.3.4. Control de aplicaciones:**

- Sistema de listas blancas y negras con categorización avanzada de software, incluyendo aplicaciones de riesgo y herramientas comunes de administración.

#### **4.3.5. Control de periféricos:**

- Gestión del uso de dispositivos conectables mediante reglas granulares y excepciones configurables.

#### **4.3.6. Interacción con otras capas de seguridad:**

- Intercambio de información con otros dispositivos de seguridad para tomar decisiones basadas en el estado del sistema y amenazas detectadas.

### **4.4. Políticas para puestos cliente**

#### **4.4.1. Control de navegación:**

- Control por categorías, con opciones de permitir, bloquear o advertir según el nivel de riesgo o política definida.



- Aplicación sin depender de extensiones de navegador ni redirecciones.

#### **4.5. Políticas para servidores**

- Listas blancas dinámicas para ejecución de software.
- Control de navegación según categorías definidas.
- Monitorización de integridad de archivos del sistema y de aplicaciones críticas.

#### **4.6. Características de protección general**

##### **4.6.1. Pre-ejecución:**

- Múltiples capas de análisis: inteligencia artificial local, firmas y heurística.
- Capacidad de respuesta en local sin depender de conexión externa.
- Escaneos en tiempo real, bajo demanda y programados.
- Capacidad de detección de amenazas avanzadas (HIPS, MTD, reputación en tiempo real).

##### **4.6.2. Post-ejecución:**

- Técnicas avanzadas de mitigación y endurecimiento del sistema frente a exploits, ransomware y ataques dirigidos.

##### **4.6.3. Post-explotación:**

- Protección ante técnicas de persistencia, elevación de privilegios y ataques basados en credenciales o scripts.

#### **4.7. Protección de Clientes**

- Soporte para sistemas Windows y macOS actuales, incluyendo arquitecturas modernas.
- Múltiples capas de protección integradas y activas simultáneamente.

#### **4.8. Protección de Servidores**

- Compatibilidad con sistemas Windows Server y Linux comunes en entornos corporativos.



## 5. Características XDR de la solución

### 5.1. Plataforma de Detección y Respuesta Ampliada (XDR)

La solución debe incorporar un sistema avanzado de Detección y Respuesta (XDR), con capacidad de consultas analíticas y operativas sobre múltiples fuentes de información. Mínimamente debe incluir:

- Amplio conjunto de consultas predefinidas categorizadas (mínimo 400), con enfoque en búsqueda de amenazas, anomalías, cumplimiento normativo, etc.
- Posibilidad de crear y editar consultas personalizadas mediante sintaxis estructurada (por ejemplo, SQL o similar).
- Ejecución de consultas directas sobre equipos Windows, macOS y Linux.
- Shell remota para intervenciones directas en los endpoints compatibles.
- Interfaz ad hoc para investigación y exploración manual de eventos de seguridad.
- Uso de filtros para seleccionar dispositivos o grupos de consulta.
- Posibilidad de compartir consultas y utilizar variables dinámicas.
- Mapeo de Indicadores de Compromiso (IoC) con la taxonomía MITRE ATT&CK.
- Exportación de resultados en formatos estándar como CSV.
- Acceso histórico a eventos del data lake de hasta 90 días, con capacidad para sistemas Windows, Mac y Linux.
- Consultas programadas y relacionales (pivoting) entre resultados.
- Integración con otras soluciones de seguridad del mismo proveedor (correo, movilidad, cloud, firewall).
- Posibilidad de consultar fuentes externas para enriquecer los resultados (IP reputation, análisis de malware, etc.).
- Registro completo de auditoría sobre consultas y acciones realizadas.
- Capacidad de uso de herramientas de inteligencia artificial para:
  - Búsqueda en lenguaje natural traducida automáticamente a lenguaje técnico.
  - Explicaciones comprensibles sobre incidentes y alertas detectadas.

### 5.2. Gestión e investigación de incidentes XDR

La plataforma debe permitir una gestión completa y eficiente de los incidentes detectados. Debe incluir:



- Funcionalidad para aislar o reincorporar dispositivos de la red.
- Exclusiones de red configurables durante el aislamiento.
- Captura de información forense en formatos estructurados (SQL, JSON).
- Envío de ficheros sospechosos al laboratorio del fabricante para su análisis mediante IA e ingeniería inversa.
- Detección de intentos de fuerza bruta y otros comportamientos anómalos.
- Acceso remoto al dispositivo incluso en estado de aislamiento.
- Consultas en vivo para obtener información contextual del ataque.
- Clasificación del estado de los ataques (nuevo, en curso, resuelto).
- Visualización gráfica de los ataques y resúmenes ejecutivos con:
  - Equipo afectado
  - Usuario implicado
  - Fecha, hora, causa raíz y detonante
- Posibilidad de asignar prioridad a cada ataque.
- Búsqueda de amenazas por múltiples atributos (nombre, hash, IP, dominio, etc.).
- Generación manual o automática de casos de amenazas.
- Detección proactiva de archivos sospechosos no bloqueados por el sistema.
- Capacidad de análisis detallado, envío al laboratorio, trazado de presencia en la red, y generación de gráficos de amenazas interactivos y actualizables.

### 5.3. Proactividad del sistema XDR

El sistema deberá ser capaz de detectar automáticamente patrones o comportamientos sospechosos y generar alertas clasificadas por:

- Nivel de riesgo
- Frecuencia
- Fecha de primera detección
- Dispositivo afectado
- Táctica o técnica relacionada (MITRE ATT&CK)
- Descripción ejecutiva del hallazgo

Las alertas deberán convertirse fácilmente en casos de investigación, que puedan gestionarse dentro de la plataforma (asignación de responsables, anotaciones, seguimiento).

### 5.4. Integración con dispositivos de seguridad perimetral

La solución XDR debe permitir integrarse con sistemas de seguridad perimetral (como firewalls) para:



- Compartir información de estado de los dispositivos y cortar el tráfico de aquellos potencialmente comprometidos.
- Aplicar reglas de segmentación basadas en la salud del endpoint.
- Compartir visibilidad de aplicaciones ejecutadas en el endpoint para su identificación en capa de red.

## 5.5. Compatibilidad con sistemas de cifrado

La solución debe incluir o integrarse con un sistema de cifrado compatible con las tecnologías nativas de los sistemas operativos (BitLocker, FileVault), permitiendo:

- Gestión centralizada de políticas de cifrado.
- Aplicación de requisitos como renovación periódica de contraseñas o PINs de acceso.

## 5.6. Interoperabilidad con soluciones de terceros

La plataforma deberá ser capaz de integrarse con otras herramientas de seguridad, productividad o infraestructura mediante conectores o APIs abiertas, incluyendo al menos:

- Soluciones de firewall líderes del mercado
- Servicios de identidad
- Sistemas de protección de correo
- Monitorización de red y tráfico
- Plataformas de productividad y nube
- Soluciones de backup y recuperación de datos

## 5.7. Análisis post-mortem de ataques

La solución debe permitir un análisis forense completo de los ataques detectados, con:

- Identificación del origen (IP, host, usuario implicado)
- Extracto técnico con todos los detalles de ejecución
- Visualización gráfica del ataque para facilitar la trazabilidad

## 6. Servicio MDR

### 6.1. Requisitos Generales

Se requiere un servicio MDR **24x7 proactivo**, proporcionado por el mismo fabricante que la solución EPP y XDR propuesta, y gestionado desde una consola unificada que centralice toda la visibilidad y gestión de seguridad.



El servicio deberá:

- Correlacionar eventos generados por los distintos módulos del fabricante (EPP, XDR, protección de servidores, etc.).
- Integrar de forma nativa la telemetría de herramientas de ciberseguridad ya desplegadas, sin necesidad de instalar agentes adicionales.
- Ser operado por centros de operaciones de seguridad distribuidos geográficamente bajo un modelo continuo de cobertura global ("follow the sun").
- Emitir alertas completas incluyendo información clave: origen, destino, tipo de amenaza, gravedad, y recomendaciones técnicas detalladas.
- Incluir intervenciones sin límite ni coste adicional en número o frecuencia durante la vigencia del contrato.
- Ofrecer no solo contención, sino también **limpieza y erradicación del malware** en los sistemas comprometidos.

### Tiempos de respuesta del servicio (objetivo y acordados):

Tipo de tiempo	Objetivo	SLA mínimo
Creación de caso	$\leq 2$ minutos desde la detección	—
Respuesta inicial	$\leq 30$ minutos desde la creación	$\leq 60$ minutos en el 90% de los casos de alta gravedad
Detección media esperada	$\sim 1$ minuto	—
Investigación media esperada	$\sim 25$ minutos	—
Remediación media esperada	$\sim 12$ minutos	—

### Términos:

- *Detección*: del evento hasta su clasificación.
- *Investigación*: hasta su notificación al responsable.
- *Remediación*: hasta acción como aislamiento o bloqueo.

## 6.2. Reconocimiento en el mercado

Se valorará positivamente que el proveedor MDR cumpla con los siguientes criterios:

- Amplia base de clientes activos en servicios MDR, preferiblemente superior a 25.000 clientes a nivel global.



- Reconocido como proveedor destacado por analistas del sector (ej. informes tipo G2 Grid).
- Resultados públicos en evaluaciones independientes (como MITRE ATT&CK Evaluations).
- Certificaciones internacionales relevantes:
  - HIPAA Type 2
  - SOC 2 Type II
  - PCI DSS

### 6.3. Supervisión y seguimiento

- Informes periódicos (semanales y mensuales) accesibles desde la consola centralizada.
- Evaluaciones del estado de salud de la plataforma con análisis de configuración y buenas prácticas, repetibles en caso de anomalías.

### 6.4. Cobertura Global 24x7

El servicio debe garantizar una cobertura completa mediante al menos **siete centros de operaciones de seguridad (SOC)** distribuidos en diferentes zonas horarias, cubriendo al menos 12 horas de diferencia entre dos de ellos.

### 6.5. Respuesta y remediación ante amenazas

#### Búsqueda proactiva de amenazas:

- Triado con inteligencia artificial y fuentes de inteligencia (como OSINT o informes de amenazas globales).
- Información continua sobre actores emergentes y vulnerabilidades críticas.

#### Respuesta activa ante incidentes:

- Aislamiento remoto de equipos
- Bloqueo de IPs a nivel de host
- Finalización de procesos maliciosos
- Revocación de sesiones activas
- Desactivación de cuentas
- Eliminación de artefactos maliciosos
- Bloqueo de indicadores (hashes)

#### Remediación posterior al incidente:

- Seguimiento en días/semanas posteriores





- Análisis forense de muestras
- Identificación de elementos comprometidos
- Revisión de registros para medidas correctivas
- Limpieza total de los sistemas afectados

## 6.6. Integración con otras herramientas

Toda la gestión, información y acciones del servicio MDR deben estar **centralizadas en la misma consola de administración** que el resto de la solución de seguridad, sin agentes adicionales.

El servicio MDR debe tener acceso completo a la consola para actuar de manera autónoma sobre endpoints, servidores y dispositivos perimetrales compatibles del mismo fabricante.

Debe permitir también la incorporación de fuentes de otros fabricantes ya desplegadas, tales como:

- Sistemas firewall
- Sistemas de gestión de identidad
- Protección de correo electrónico
- Soluciones en la nube
- Herramientas de detección en red (NDR)
- Soluciones de backup
- Plataformas de productividad (Microsoft 365, Google Workspace, etc.)

## 7. Licencias

Se incluirán todas las **licencias necesarias** para garantizar el funcionamiento completo de la solución, cubriendo tanto los requisitos obligatorios como cualquier funcionalidad adicional ofrecida.

Todas las licencias, funcionalidades, suscripciones y derechos de uso deberán tener una duración mínima de **tres (3) años** desde la fecha de la puesta en servicio del sistema, sin limitaciones de funcionalidad ni necesidad de renovación intermedia.

- Las renovaciones de licencia deberán contemplar la **ampliación proporcional del periodo de garantía**.
- Cualquier funcionalidad ofertada deberá estar incluida sin requerir pagos adicionales por características individuales.
- No se aceptarán propuestas con licencias limitadas en funcionalidad o alcance respecto a lo especificado en este pliego.



## 8. Empresa implantadora

Se valorará que la empresa tenga un **nivel de certificación alto en la tecnología propuesta**, acorde con los requisitos del fabricante, como por ejemplo certificaciones de tipo *Gold* o *Platinum*, o equivalentes en función del modelo de partnership del fabricante.

La empresa implantadora deberá disponer de técnicos propios que puedan prestar servicios presenciales en las fases clave del proyecto:

- Implantación de la solución
- Reuniones de seguimiento
- Atención a incidencias críticas

La empresa adjudicataria deberá contar con implantación local en al menos dos islas de la Comunidad Autónoma de Canarias, disponiendo de personal propio acreditado y certificado en la tecnología ofertada para garantizar una correcta implantación, soporte y mantenimiento de la solución.

## 9. Configuración, instalación y puesta en servicio

Con el objetivo de asegurar una implantación efectiva, segura y sin interrupciones de la nueva infraestructura de seguridad perimetral y protección de endpoints, se detallan los pasos y requisitos a cumplir por el adjudicatario:

### 9.1. Planificación y Preparación

- **Análisis del entorno actual de red**, identificando puntos críticos, dependencias tecnológicas y requerimientos personalizados.
- **Desarrollo de un plan de implementación** detallado con cronograma, recursos asignados, fases y medidas de contingencia.
- **Revisión de pre-requisitos técnicos**, garantizando compatibilidad con infraestructuras existentes y disponibilidad de recursos.

### 9.2. Configuración de hardware y red

- **Asistencia en el montaje físico** de los dispositivos, verificación de conexiones e integración en rack.
- **Configuración de red y políticas de seguridad** según el diseño aprobado:
  - Asignación de interfaces, direcciones IP, segmentación.



- o Reglas de firewall iniciales, configuración de IPS y control de acceso.
- o Configuración de túneles VPN (SSL y/o IPsec) y validación de conexiones.
- **Integración con sistemas corporativos:**
  - o Sincronización con servicios de directorio locales y en la nube (AD/Azure AD u otros).
  - o Gestión centralizada de políticas y usuarios.

### 9.3. Instalación y configuración de software

- **Actualización de firmware y software a versiones estables más recientes.**
- **Configuración de actualización automática** con control sobre versiones, parches y revisiones críticas.
- **Implementación de funciones avanzadas:**
  - o Protección avanzada de endpoints
  - o Análisis de amenazas
  - o Sandboxing
  - o Inspección de tráfico cifrado (SSL/TLS)
  - o Balanceo de carga y calidad de servicio (QoS)

### 9.4. Puesta en servicio

- **Pruebas funcionales y de carga** para validar conectividad, políticas aplicadas, rendimiento y alta disponibilidad.
- **Monitorización inicial** con ajustes de parámetros y configuración de alertas, informes y notificaciones.
- **Documentación técnica completa** de la solución implementada.

### 9.5. Capacitación

**Formación inicial al personal técnico de GESPLAN**, incluyendo:

- **Sesiones teóricas y prácticas** sobre gestión de la consola, configuración, respuesta ante incidentes y mantenimiento.
- **Simulación de escenarios reales** para consolidar conocimientos y respuestas operativas.
- **Materiales de formación actualizados**, incluyendo manuales, guías y acceso a recursos formativos online.

**Capacitación continua:**

- Actualización de conocimientos ante nuevas funcionalidades o mejoras.



- Punto de contacto técnico para resolución de dudas o refuerzo puntual.

## 9.6. Soporte y mantenimiento

- **Administración integral de la solución** por parte del adjudicatario durante la vigencia del contrato:
  - Soporte proactivo y mantenimiento preventivo.
  - Gestión de actualizaciones, configuración y optimización continua.
  - Supervisión de amenazas y generación de informes.
- **Acceso garantizado a actualizaciones de producto y bases de datos de amenazas.**
- **Soporte técnico del fabricante mediante asistencia remota**, con intervención presencial cuando sea necesaria.
- **Implantación local del adjudicatario en al menos dos islas del archipiélago donde se instale la solución**, con personal técnico cualificado **disponible para actuación in situ**.
  - No se aceptará la **subcontratación puntual** de terceros para cumplir esta condición. La empresa local deberá estar integrada estructuralmente en el servicio.
- El adjudicatario será el **único punto de interlocución con el cliente**, actuando como coordinador técnico ante cualquier incidencia o consulta con el fabricante.
- El servicio de soporte, mantenimiento correctivo, preventivo y evolutivo deberá cubrir un periodo mínimo de **tres (3) años**, contados desde la aceptación definitiva de la solución por parte de GESPLAN. Durante dicho periodo, el adjudicatario deberá garantizar el acceso a actualizaciones de seguridad, mejoras de funcionalidad, resolución de incidencias y atención técnica especializada sin coste adicional.



## 10. Confidencialidad

Con el fin de garantizar la confidencialidad de la información de GESPLAN, si por motivos de la prestación de los servicios objeto del contrato los técnicos de la empresa adjudicataria tuviesen que acceder a información de carácter personal y/o confidencial, la empresa adjudicataria deberá suscribir un acuerdo de confidencialidad que le comprometa durante la vigencia del contrato de soporte a tratar los datos de acceso a los sistemas corporativos de GESPLAN y a los datos en ellos albergados con la debida confidencialidad, observando siempre el secreto profesional, y en cualquier caso asegurando el cumplimiento de la normativa de aplicación para el tratamiento de la información de carácter personal.

## 11. Garantía

El adjudicatario deberá proporcionar una garantía mínima de **tres (3) años** sobre el hardware suministrado, así como sobre el correcto funcionamiento de toda la solución implementada, incluyendo sus componentes software, configuración, integración y personalización.

Durante dicho periodo de garantía, deberá cubrirse la reparación o sustitución de los elementos defectuosos sin coste para GESPLAN, así como el mantenimiento evolutivo y correctivo de la solución instalada.

A fecha de firma electrónica en Las Palmas de Gran Canaria

