

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 de calidad y conformidad: ISO 9001, FIPS 140-2/3, IPv6 Ready, CE, FCC, u otras equivalentes según normativa del país de origen.

Nota: No se exigirá que todos los certificados estén presentes simultáneamente, pero sí que se cumplan al menos dos de los anteriormente mencionados.

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 ≥ 40 Gbps en tráfico mixto (IMIX).
- Rendimiento de IPS ≥ 10 Gbps.
- VPN IPsec ≥ 10 Gbps.
- Latencia máxima permitida en pruebas UDP de 64 bytes ≤ 10 μ s.
- Capacidad de conexiones simultáneas: ≥ 5 millones.
- Conexiones por segundo: ≥ 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	≤ 2 minutos desde la detección	—
Respuesta inicial	≤ 30 minutos desde la creación	≤ 60 minutos en el 90% de los casos de alta gravedad
Detección media esperada	~1 minuto	—
Investigación media esperada	~25 minutos	—
Remediación media esperada	~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.

- 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

La empresa implantadora deberá cumplir al menos con las siguientes certificaciones vigentes:

- UNE-EN ISO 9001:2015 (Gestión de la calidad)
- UNE-EN ISO 14001:2015 (Gestión ambiental)
- UNE-ISO/IEC 20000-1:2018 (Gestión de servicios TI)
- UNE-EN ISO/IEC 27001:2023 (Gestión de seguridad de la información)
- Registro de Huella de Carbono actualizado
- Cumplimiento con el Reglamento General de Protección de Datos (RGPD)
- Conformidad con el Esquema Nacional de Seguridad (ENS)
- Adecuación al marco de la Directiva NIS 2

Adicionalmente, 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

Los técnicos que atiendan los servicios deberán estar **debidamente certificados en la tecnología** y productos propuestos, lo que deberá acreditarse documentalmente.

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.
 - Reglas de firewall iniciales, configuración de IPS y control de acceso.
 - Configuración de túneles VPN (SSL y/o IPsec) y validación de conexiones.
- **Integración con sistemas corporativos:**
 - Sincronización con servicios de directorio locales y en la nube (AD/Azure AD u otros).
 - 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:**
 - Protección avanzada de endpoints
 - Análisis de amenazas
 - Sandboxing
 - Inspección de tráfico cifrado (SSL/TLS)
 - 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.

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.

A fecha de firma electrónica en Las Palmas de Gran Canaria