Expediente P.O.07.24

Pliego de Prescripciones Técnicas para la adquisición de equipos físicos y servicios de ciberseguridad perimetral para la Autoridad Portuaria de Baleares

Contenido

1 Antecedentes

La Autoridad Portuaria de Baleares (en adelante APB) está actualmente en proceso de certificación conforme al Esquema Nacional de Seguridad (ENS). Como parte esencial de este proceso, se requiere implementar la medida de seguridad de "perímetro seguro". Por consiguiente, es imprescindible adquirir equipos especializados, entre ellos firewalls, así como llevar a cabo su instalación, configuración, puesta en marcha, gestión y mantenimiento para garantizar el cumplimiento óptimo de dicha medida de seguridad.

2 Objeto del contrato

El objeto de este contrato consiste en el suministro, instalación, configuración, puesta en marcha, gestión y mantenimiento del sistema de protección perimetral de red para la APB.

El suministro, instalación, configuración y puesta en marcha se deberá realizar en las diferentes sedes de la APB (Palma, Maó, Eivissa, Alcúdia y la Savina), de conformidad con las especificaciones contenidas en el presente pliego de prescripciones técnicas.

La contratación incluye, así mismo, la contratación de las suscripciones a soportes y servicios de seguridad, herramientas de monitorización, gestión y control de acceso del sistema de protección perimetral, así como la formación, soporte técnico y consultoría, detallados en el presente pliego.

3 Documentación a disposición del adjudicatario

La APB facilitará a la empresa adjudicataria toda la documentación necesaria y disponible para la correcta ejecución del contrato.

Dicha información estará sometida a compromiso de confidencialidad por parte de la empresa adjudicataria y de su personal. La intención de la APB es que en ningún caso salga documentación, especialmente en soporte papel, de la APB para realizar las tareas establecidas y derivadas de este Pliego.

4 Legislación y normas que regirán los trabajos a realizar

El desarrollo de los trabajos solicitados en el presente pliego de prescripciones técnicas se realizará al amparo de la siguiente normativa, que se entiende de obligado cumplimiento:

- Procedimiento administrativo electrónico
  - Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
  - Real Decreto-ley 11/2018, de 31 de agosto, por el que se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
  - Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas.
  - Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.
- Contratación pública
  - Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo, (UE) 2014/23 y (UE) 2014/24, de 26 de febrero de 2014.

- Seguridad y protección de datos
  - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  - Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
  - Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad).
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información.
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
  - Instrucciones Técnicas de Seguridad y las Guías de Seguridad derivadas del Esquema Nacional de Seguridad.
- Ley de Prevención de Riesgos Laborales, Ley 31/1995 (BOE nº 269 de 10 de noviembre) y todos los Reales Decretos que la regulan, en especial el 1627/1997.
- Normas NTE.
- Normas UNE.
- Normas DIN e ISO.
- Cualquier otra normativa, que se publique o desarrolle durante la duración del contrato, y sea de obligado cumplimiento a las Administraciones Públicas, y en particular, a la APB.

Asimismo, quedará incluida en el ámbito del proyecto cualquier adaptación -sea desarrollo o cualquier otro tipo de trabajo- a la legislación que pudiera surgir durante el desarrollo del proyecto y el posterior periodo de garantía.

5 Descripción de las tareas objeto del contrato

Con carácter enunciativo y no exhaustivo, el contrato incluye los suministros y servicios que se detallan a continuación.

5.1 Sistema de protección perimetral de red.

La APB quiere implantar en sus distintas sedes (Palma, Maó, Eivissa, Alcúdia y la Savina) un sistema de protección perimetral de red de nueva generación (*Next Generation Firewall (NGFW)*) compuesto por dos capas separadas (externa e interna). El firewall exterior funcionará como frontera entre las redes externas a la APB y las redes DMZ y el firewall interno servirá como frontera entre las redes DMZ e internas.

En este sentido, se incluye a continuación el número de firewalls que se requieren en las distintas sedes de la APB para implantar el sistema de protección perimetral de red:

- Palma: 4 firewalls tipo A (2 para el CPD principal y 2 para el CPD de backup).
- Maó: 2 firewalls tipo B.
- Eivissa: 2 firewalls tipo B.
- Alcúdia: 2 firewalls tipo C.
- La Savina: 2 firewalls tipo C.

Los requisitos mínimos de cada una de las capas separadas (externa e interna) y de los tipos definidos (tipo A, tipo B y tipo C), se describen en los siguientes apartados. También se incluyen los servicios que se deben proporcionar referidos a cada uno de los equipos, así como las herramientas de monitorización, gestión y de control de acceso a suministrar.

Requisito obligatorio

Es un requisito que los equipos ofertados estén publicados en la Guía CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) y sean de categoría ENS ALTA.

Además de los firewalls indicados anteriormente, se incluye dentro del alcance del contrato:

- Todo el hardware y el software necesario para la implantación del sistema de protección perimetral de red.
- Todas las licencias y suscripciones necesarias para activar, así como, todas las funcionalidades asociadas a los requerimientos obligatorios que se indican en este pliego de prescripciones técnicas.
- El suministro, instalación, configuración, puesta en marcha, gestión y mantenimiento de todo el sistema de protección perimetral de red de la APB que, se deberá realizar, según las indicaciones de la APB.
- La gestión del proyecto.

5.1.1 Requisitos y servicios avanzados de seguridad y tecnología comunes a todos los NGFW.

Los equipos ofertados en esta contratación deben cumplir los siguientes requisitos mínimos comunes:

- A nivel de integración debe incluir una controladora LAN con soporte como mínimo de 32 conmutadores.
- A nivel de integración debe incluir una controladora WLAN para dar soporte como mínimo a 128/64 puntos de acceso.
- Deberá tener una integración nativa con una plataforma de gestión ZTNA en cloud, ofreciendo:
  1. Intercambio de etiquetas ZTNA para acceso en políticas de firewall locales, accesos VPN SSL y accesos remotos por ZTNA proxy.
  2. Telemetría con información de vulnerabilidades de los endpoints.
  3. Intercambio de etiquetas ZTNA con todos los Firewalls.
  4. Mecanismos de cuarentena automática de dispositivo mediante agente ZTNA por políticas de automatización.
- Los equipos no deben tener límites de uso de interfaces en SDWAN, y entregar toda la capacidad de ancho de banda sin licencias adicionales.
- Como máximo ocuparan 2xRU.

- Equipamiento debe soportar HA con sincronía de configuración y gestión única.
- La gestión con usuarios locales debe estar protegida mediante mecanismos de doble factor con notificaciones push a aplicación móvil del mismo fabricante.
- El equipamiento debe soportar funcionalidades de "IN LINE CASB" y DLP sin necesidad de añadir licencias adicionales ni soluciones de terceros.
- Debe incluir firmas industriales para realizar funciones de IPS y control de aplicaciones con soporte de más de 3.000 firmas dedicadas a protocolos y aplicaciones industriales.
- Capacidad de parcheo virtual para dispositivos IOT/OT con capacidad de detección dispositivos y aplicaciones vulnerables y remediación protección del mismo.
- Todos los firewalls deberán disponer de un disco duro interno para el almacenaje de logs de larga duración en local para disponer de una alternativa en caso de indisponibilidad de la herramienta de consolidación de eventos.
- El equipamiento debe incluir subscripción para el soporte de Sandbox Cloud durante toda la duración del contrato.

Los servicios mínimos avanzados de seguridad y tecnología que deben incluir todos los NGFW son:

- **Seguridad de Red y Archivos**: Protección contra amenazas basadas en red y archivos. Esto incluye un sistema de Prevención de Intrusiones (IPS) con modelos de IAM para inspección profunda de paquetes/SSL, detección y bloqueo de contenido malicioso, y aplicación de parches virtuales. Además, deben incluir servicios Anti-Malware para defensa contra amenazas basadas en archivos, que abarcan tanto antivirus como sandboxing de archivos, con actualizaciones en tiempo real.
- **Control de Aplicaciones y Seguridad Web/DNS**: Protección contra amenazas web, incluyendo amenazas basadas en DNS, URLs maliciosas, y comunicaciones de botnet/mando y control. El filtrado de DNS debe ofrecer visibilidad completa del tráfico DNS bloqueando dominios de alto riesgo, protección contra túneles de DNS, infiltración de DNS, identificación de servidores C2 y algoritmos de generación de dominios (DGA). El filtrado de URL que utilice una base de datos de más de 300 millones de URLs para identificar y bloquear enlaces a sitios y cargas maliciosas.
- **Seguridad SaaS y de Datos**: Posibilidad de abordar múltiples casos de uso de seguridad en cuanto al uso de aplicaciones y la seguridad general de los datos. Esto debe incluir Prevención de Fuga de Datos (DLP) para garantizar la visibilidad, gestión y protección de datos (incluyendo el bloqueo de exfiltración) en redes, nubes y usuarios, y servicio de Broker de Acceso a la Seguridad en la Nube (CASB) para proteger los datos en movimiento, en reposo y en la nube.
- **Prevención de Amenazas de Día Cero**: Prevención en tiempo real de amenazas desconocidas a través de la prevención de malware en línea, incluyendo un servicio avanzado de sandbox para analizar y bloquear archivos desconocidos, proporcionando protección contra amenazas sofisticadas y de día cero en todos los NGFW.
- **Seguridad OT**: Detección de OT, correlación de vulnerabilidades de OT, parcheo virtual, firmas de OT y decodificadores de protocolos específicos de la industria para una defensa robusta de entornos y dispositivos OT.
- **Soporte del equipamiento**: se incluye soporte avanzado sobre el equipamiento, así como sobre las herramientas de monitorización, gestión y de control de acceso de los NGFW, durante **dos años,** que debe cumplir:

- Soporte ofrecido por el fabricante 24x7x365 que incluya sustitución de equipo en caso de avería para el equipamiento y productos.
- Actualizaciones de firmware y software.
- Portal de gestión de activos.
- Soporte web y telefónico.
- Apertura de casos para incidencias en versiones, actualizaciones, bugs, etc.
- Tiempos de respuesta:
  - 1 hora para incidencias críticas.
  - Día siguiente laborable para incidencias no críticas.

5.1.2 Equipos TIPO A.

5.1.2.1 Características de los equipos TIPO A.

Además de las características comunes a todos los firewalls, los equipos cortafuegos TIPO A a suministrar deberán contar con las siguientes características específicas:

- **Firewall de Nueva Generación (NGFW)**: Debe incluir servicios de seguridad de potenciados por IA, integrados de forma nativa en el NGFW, de manera que asegure el contenido web y proteja las redes contra ransomware y ataques cibernéticos sofisticados. La inspección SSL en tiempo real debe proporcionar total visibilidad de usuarios, dispositivos y aplicaciones.
- **Segmentación**: Adaptación dinámica a cualquier topología de red, ofreciendo seguridad de extremo a extremo. Segmentación VXLAN ultraescalable y de baja latencia, y prevención de movimientos laterales en la red con protección avanzada.
- **SD-WAN Seguro**: Transformación y aseguramiento de las WANs, ofreciendo calidad superior de experiencia y una postura de seguridad efectiva para modelos de trabajo remoto, SD-Branch y casos de uso de WAN basados en la nube.
- **Seguridad Móvil para 4G, 5G e IoT**: CGNAT acelerado por SPU y opciones de migración a IPv6, seguridad de acceso RAN y gateway de seguridad (SecGW) con protección total de amenazas e inspección de GTP-U.
- **SPU y ASIC**: Impulsado por la Unidad de Procesamiento de Seguridad (SPU), este dispositivo debe ofrecer un mínimo de 520Gbps para detectar y bloquear amenazas emergentes sin convertirse en un cuello de botella de rendimiento. Debe incluir procesadores de red NP7 y los procesadores de contenido CP9 operando en línea, con aceleración de configuración de sesión y latencia ultra baja, rendimiento líder en la industria para VPN y VXLAN, y procesamiento acelerado de SSL y funciones de seguridad.
- Interfaces y Módulos:
  - 16 puertos GE RJ45 acelerados por hardware.
  - 8 ranuras GE SFP aceleradas por hardware.
  - 12 ranuras SFP28 de 25 GE / SFP+ de 10 GE / GE SFP aceleradas por hardware.
  - 4 ranuras QSFP28 de 100 GE / QSFP+ de 40 GE aceleradas por hardware.
  - 2 puertos de gestión GE RJ45.
  - 2 ranuras HA SFP+ de 10 GE / GE SFP.
  - 1 puerto USB 3.0.
  - 1 puerto de consola RJ45.
  - Almacenamiento a bordo: 2x 1TB NVMe SSD.
  - Transceptores incluidos: 2x SFP+ (SR 10 GE).

    - Módulo de Plataforma de Confianza (TPM): Debe contar con un módulo dedicado que refuerza los dispositivos de red físicos generando, almacenando y autenticando claves criptográficas. Así mismo, debe disponer de mecanismos de seguridad basados en hardware para protección contra software malicioso y ataques de phishing.
    - Conectividad de 100 GE: Múltiples ranuras QSFP28 de 100 GE.
- Rendimiento del Sistema – Tráfico Empresarial:
    - Rendimiento de IPS: 22 Gbps.
    - Rendimiento NGFW: 17 Gbps.
    - Rendimiento de Protección contra Amenazas: 15 Gbps.
- Rendimiento y Capacidad del Sistema:
    - Rendimiento del Firewall IPv4 (1518 / 512 / 64 byte, UDP): 198 / 197 / 140 Gbps.
    - Rendimiento del Firewall IPv6 (1518 / 512 / 86 byte, UDP): 198 / 197 / 140 Gbps.
    - Latencia del Firewall (64 byte, UDP): 3.22 µs.
    - Rendimiento del Firewall (Paquetes por Segundo): 210 Mpps.
    - Sesiones Concurrentes (TCP): 12 millones / 40 millones.
    - Nuevas Sesiones/Segundo (TCP): 750.000 / 2 millones.
    - Políticas de Firewall: 100.000.
- Capacidades de VPN y SSL:
    - Rendimiento de VPN IPsec (512 byte): 55 Gbps.
    - Túneles VPN de Gateway-a-Gateway IPsec: 20.000.
    - Túneles VPN de Cliente-a-Gateway IPsec: 100.000.
    - Rendimiento de SSL-VPN: 11 Gbps.
    - Usuarios Concurrentes de SSL-VPN (Máximo Recomendado, Modo Túnel): 10.000.
    - Rendimiento de Inspección SSL (IPS, HTTPS promedio): 12 Gbps.
    - CPS de Inspección SSL (IPS, HTTPS promedio): 9.500.
    - Sesiones Concurrentes de Inspección SSL (IPS, HTTPS promedio): 1.3 millones.
- Control de Aplicaciones y Rendimiento de CAPWAP:
    - Rendimiento de Control de Aplicaciones (HTTP 64K): 34 Gbps.
    - Rendimiento CAPWAP (HTTP 64K): 65 Gbps.
- Dimensiones y Potencia:
    - Formato: Montaje en rack, 2RU.
    - Fuente de alimentación AC: 100–240VAC, 50/60 Hz.
    - Consumo de energía (Promedio/Máximo): 410.9 W / 459.1 W.
    - Disipación de calor: 1565.53 BTU/h.
    - Fuentes de alimentación redundantes y cambiables en caliente.
- Entorno Operativo y Certificaciones:
    - Temperatura operativa: 32°–104°F (0°–40°C).
    - Temperatura de almacenamiento: -31°–158°F (-35°–70°C).
    - Humedad: 10%–90% sin condensación.
    - Nivel de ruido: 62.74 dBA.
    - Flujo de aire forzado de lado a lado y de frente a atrás.
    - Altitud operativa: hasta 7400 pies (2250 m).
    - Cumplimiento: FCC Parte 15 Clase A, RCM, VCCI, CE, UL/cUL, CB.

5.1.2.2 Soporte de seguridad para los equipos de TIPO A.

Para los equipos de tipo A se incluirá la suscripción a las siguientes licencias de soportes de seguridad (soporte directo del fabricante) durante **dos años:**

- **Soporte de seguridad avanzado para equipo de tipo A** que incluya:
  - Protección Unificada de amenazas (UTP) (sistema de prevención de intrusiones (IPS), protección avanzada contra Malware, control de aplicaciones, filtrado URL, DNS y Video, servicio AntiSpam y servicio de soporte avanzado)
- **Soporte de seguridad avanzado para entornos de tecnología operativa (OT) para equipo tipo A** que incluya**:**
  - Paneles de control de OT y reportes de cumplimiento, detección de aplicaciones y servicios de OT, correlación de vulnerabilidades de OT, parcheado virtual de OT, firmas de OT – reglas de control de aplicaciones y IPS.

5.1.3 Equipos TIPO B.

5.1.3.1 Características de los equipos TIPO B.

Además de las características comunes a todos los firewalls, los equipos cortafuegos TIPO B a suministrar deberán cumplir con las siguientes características específicas:

- **Firewall de Nueva Generación (NGFW)**: debe incluir funcionalidades que permitan proteger contra ransomware y ciberataques avanzados. Inspección SSL en tiempo real para una visibilidad completa.
- **SD-WAN Seguro**: Transformación y aseguramiento de las WANs, proporcionando una experiencia de calidad superior y una postura de seguridad efectiva para diferentes modelos de trabajo y casos de uso.
- **ZTNA Universal**: Control de acceso a aplicaciones independientemente de la ubicación del usuario o la aplicación, con autenticaciones extensas y cumplimiento de políticas.
- **Segmentación**: Adaptación dinámica a cualquier topología de red, con segmentación VXLAN y prevención de movimientos laterales en la red gracias a la protección avanzada.
- **SPU y ASIC**: Impulsados por la Unidad de Procesamiento de Seguridad (SPU), el dispositivo debe ofrecer un mínimo de 520Gbps para detectar y bloquear amenazas emergentes sin convertirse en un cuello de botella de rendimiento. Debe incluir procesadores de red NP7 y los procesadores de contenido CP9 operando en línea, con aceleración de configuración de sesión y latencia ultra baja, rendimiento líder en la industria para VPN y VXLAN, y procesamiento acelerado de SSL y funciones de seguridad.
- Interfaces y Módulos:
  - 16 interfaces GE RJ45 aceleradas por hardware.
  - 8 ranuras GE SFP aceleradas por hardware.
  - 4 ranuras SFP+ de 10GE / GE SFP aceleradas por hardware.
  - 4 ranuras SFP28 de 25GE / SFP+ de 10GE de ultra baja latencia.
  - 2 puertos GE RJ45 MGMT/HA.
  - 2 puertos USB.
  - 1 puerto de consola RJ45.
  - Almacenamiento a bordo: 2x 240 GB SSD.

    - Módulo de Plataforma de Confianza (TPM): módulo dedicado que refuerza los dispositivos de red físicos generando, almacenando y autenticando claves criptográficas, proporcionando protección contra software malicioso y ataques de phishing.
    - Seguridad en la Capa de Acceso: Protocolo que permita converger la seguridad y el acceso a la red.
- Rendimiento del Sistema – Tráfico Empresarial:
    - Rendimiento de IPS: 14 Gbps.
    - Rendimiento NGFW: 11.5 Gbps.
    - Rendimiento de Protección contra Amenazas: 10.5 Gbps.
- Rendimiento y Capacidad del Sistema:
    - Rendimiento del Firewall IPv4 / IPv6 (1518 / 512 / 64 byte, UDP): 139 / 137.5 / 70 Gbps.
    - Latencia del Firewall (64 byte, UDP): 4.12 µs / 2.5 µs.
    - Rendimiento del Firewall (Paquetes por Segundo): 105 Mpps.
    - Sesiones Concurrentes (TCP): 8 millones.
    - Nuevas Sesiones/Segundo (TCP): 550.000.
    - Políticas de Firewall: 10.000.
- Capacidades de VPN y SSL:
    - Rendimiento de VPN IPsec (512 byte): 55 Gbps.
    - Túneles VPN de Gateway-a-Gateway IPsec: 2.000.
    - Túneles VPN de Cliente-a-Gateway IPsec: 50.000.
    - Rendimiento de SSL-VPN: 4.3 Gbps.
    - Usuarios Concurrentes de SSL-VPN (Máximo Recomendado, Modo Túnel): 10.000.
    - Rendimiento de Inspección SSL (IPS, HTTPS promedio): 9 Gbps.
- Control de Aplicaciones y Rendimiento de CAPWAP:
    - Rendimiento de Control de Aplicaciones (HTTP 64K): 32 Gbps.
    - Rendimiento CAPWAP (HTTP 64K): 64.5 Gbps.
- Dimensiones y Potencia:
    - Formato: Montaje en rack, 1RU.
    - Consumo de energía (Promedio/Máximo): 169 W / 255 W.
- Entorno Operativo y Certificaciones:
    - Temperatura operativa: 32°–104°F (0°–40°C).
    - Temperatura de almacenamiento: -31°–158°F (-35°–70°C).
    - Humedad: 5%–90% sin condensación.
    - Nivel de ruido: 55 dBA.
    - Flujo de aire de lado a lado y de frente a atrás.
    - Altitud operativa: hasta 10.000 pies (3048 m).
    - Cumplimiento: FCC Parte 15 Clase A, RCM, VCCI, CE, UL/cUL, CB.

5.1.3.2 Soporte de seguridad para los equipos de TIPO B.

Para los equipos de TIPO B se incluirá la suscripción a las siguientes licencias de soportes de seguridad (soporte directo del fabricante) durante **dos años**:

- **Soporte de seguridad avanzado para equipo de tipo B** que incluya:

- Protección Unificada de amenazas (UTP) (sistema de prevención de intrusiones (IPS), protección avanzada contra Malware, control de aplicaciones, filtrado URL, DNS y Video, servicio AntiSpam y servicio de soporte avanzado)

- **Soporte de seguridad avanzado para entornos de tecnología operativa (OT) para equipo tipo B** que incluya:
  - Paneles de control de OT y reportes de cumplimiento, detección de aplicaciones y servicios de OT, correlación de vulnerabilidades de OT, parcheado virtual de OT, firmas de OT – reglas de control de aplicaciones y IPS.

5.1.4 Equipos TIPO C

5.1.4.1 Características de los equipos TIPO C.

Además de las características comunes a todos los firewalls, los equipos cortafuegos TIPO C a suministrar deberán cumplir con las siguientes características específicas:

- **Firewall de Nueva Generación (NGFW):** debe incluir servicios de seguridad de protección de web, contenido y dispositivos, y debe proporcionar protección contra ransomware y ciberataques sofisticados. La inspección SSL en tiempo real brinda visibilidad completa en usuarios, dispositivos y aplicaciones.
- **SD-WAN Seguro**: Transformación y aseguramiento de las WANs, ofreciendo una calidad de experiencia superior y una postura de seguridad efectiva para modelos de trabajo remoto, SD-Branch y casos de uso de WAN basados en la nube.
- **ZTNA Universal**: Control de acceso a aplicaciones con autenticaciones exhaustivas y cumplimiento de políticas, ofreciendo acceso basado en agentes o sin agentes para invitados o BYOD.
- **Segmentación**: Adaptación dinámica a cualquier topología de red, con segmentación VXLAN de baja latencia y prevención de movimientos laterales en la red gracias a la protección avanzada.
- **SPU y ASIC**: Impulsado por la Unidad de Procesamiento de Seguridad (SPU), este dispositivo brinda un rendimiento de un mínimo de 520Gbps para detectar y bloquear amenazas sin ser un cuello de botella. El ASIC SOC4 debe combinar con un CPU basado en RISC con la SPU para un buen rendimiento en identificación y dirección de aplicaciones, aceleración de VPN IPsec, seguridad NGFW y inspección profunda de SSL, y conectividad acelerada e integrada para transformación de SD-Branch, todo esto con una reducción significativa en el consumo de energía.
- Interfaces y Módulos:
  - 16 interfaces GE RJ45 aceleradas por hardware.
  - 8 ranuras GE SFP aceleradas por hardware.
  - 4 ranuras SFP+ de 10GE / GE SFP aceleradas por hardware.
  - 4 ranuras SFP28 de 25GE / SFP+ de 10GE de ultra baja latencia.
  - 2 puertos GE RJ45 MGMT/HA.
  - 2 puertos USB.
  - 1 puerto de consola RJ45.
  - Almacenamiento a bordo: 2x 240 GB SSD.
  - Módulo de Plataforma de Confianza (TPM): Debe incluir un módulo dedicado que refuerza los dispositivos de red físicos generando, almacenando y autenticando claves criptográficas, proporcionando protección contra software malicioso y ataques de phishing.

  - Seguridad en la Capa de Acceso: Debe disponer del protocolo para permitir converger la seguridad y el acceso a la red. Los puertos habilitados pueden ser reconfigurados como puertos regulares según sea necesario.
- Rendimiento del Sistema – Tráfico Empresarial:
  - Rendimiento de IPS: 14 Gbps.
  - Rendimiento NGFW: 11.5 Gbps.
  - Rendimiento de Protección contra Amenazas: 10.5 Gbps.
- Rendimiento y Capacidad del Sistema:
  - Rendimiento del Firewall IPv4 / IPv6 (1518 / 512 / 64 byte, UDP): 139 / 137.5 / 70 Gbps.
  - Latencia del Firewall (64 byte, UDP): 4.12 µs / 2.5 µs*.
  - Rendimiento del Firewall (Paquetes por Segundo): 105 Mpps.
  - Sesiones Concurrentes (TCP): 8 millones.
  - Nuevas Sesiones/Segundo (TCP): 550.000.
  - Políticas de Firewall: 10.000.
- Capacidades de VPN y SSL:
  - Rendimiento de VPN IPsec (512 byte): 55 Gbps.
  - Túneles VPN de Gateway-a-Gateway IPsec: 2.000.
  - Túneles VPN de Cliente-a-Gateway IPsec: 50.000.
  - Rendimiento de SSL-VPN: 4.3 Gbps.
  - Usuarios Concurrentes de SSL-VPN (Máximo Recomendado, Modo Túnel): 10.000.
  - Rendimiento de Inspección SSL (IPS, HTTPS promedio): 9 Gbps.
- Control de Aplicaciones y Rendimiento de CAPWAP:
  - Rendimiento de Control de Aplicaciones (HTTP 64K): 32 Gbps.
  - Rendimiento CAPWAP (HTTP 64K): 64.5 Gbps.
- Dimensiones y Potencia:
  - Formato: Montaje en rack, 1RU.
  - Consumo de energía (Promedio/Máximo): 169 W / 255 W.
- Entorno Operativo y Certificaciones:
  - Temperatura operativa: 32°–104°F (0°–40°C).
  - Temperatura de almacenamiento: -31°–158°F (-35°–70°C).
  - Humedad: 5%–90% sin condensación.
  - Nivel de ruido: 55 dBA.
  - Flujo de aire de lado a lado y de frente a atrás.
  - Altitud operativa: hasta 10.000 pies (3048 m).
  - Cumplimiento: FCC Parte 15 Clase A, RCM, VCCI, CE, UL/cUL, CB.

5.1.4.2 Servicios de seguridad para los equipos de TIPO C.

Para los equipos de tipo C se incluirá la suscripción a las siguientes licencias de soportes de seguridad durante (soporte directo del fabricante) **dos años**:

- **Soporte de seguridad avanzado para equipo de tipo C** que incluya:
  - Protección Unificada de amenazas (UTP) (sistema de prevención de intrusiones (IPS), protección avanzada contra Malware, control de aplicaciones, filtrado URL, DNS y Video, servicio AntiSpam y servicio de soporte avanzado)
- **Soporte de seguridad avanzado para entornos de tecnología operativa (OT) para equipo tipo C** que incluya:

- Paneles de control de OT y reportes de cumplimiento, detección de aplicaciones y servicios de OT, correlación de vulnerabilidades de OT, parcheado virtual de OT, firmas de OT – reglas de control de aplicaciones y IPS.

5.1.5 Herramientas de monitorización y gestión de los NGFW.

5.1.5.1 Herramienta de gestión de registros.

Se incluye dentro del alcance de los elementos a contratar el de una herramienta de análisis y gestión de la seguridad, del mimo fabricante que los firewalls, que permita maximizar la inteligencia operativa para ampliar la capacidad analítica diaria y aprovechar al máximo la recopilación de logs.

Las características principales de la solución son:

- Permite la ingestión de logs de todos los firewalls, dispositivos con agente ZTNA y herramienta de PAM.
- Dispone de informes predefinidos y capacidad de crear informes totalmente personalizados en contenido e idioma
- Permite crear gestión delegada en modo multi-tenant
- Permite paneles de visibilidad.
- Soporta la respuesta de incidentes de manera automática.
- Permite la gestión de registros, que permita agregar un mínimo de 25 GB de logs por día.

Además, incluye un paquete de servicios (con soporte directo del fabricante) con las siguientes funcionalidades, a proporcionar durante **dos años**:

- **Soporte avanzado** (un mínimo de 26 GB logs por día) que incluya asistencia técnica de soporte a usuarios, así como, actualizaciones de software.
- **Servicio de automatización de seguridad** (un mínimo de 26GB logs por día) que incluya: informes detallados, manejadores de eventos, reglas de correlación SIEM para detección avanzada de amenazas, libretos SOAR, etc.
- **Servicio de detección de IOC y brotes** (un mínimo de 26GB logs por día): servicio que permita proteger la red contra amenazas emergentes y brotes.

5.1.5.2 Orquestador de Firewalls.

Se incluye dentro del alcance de los elementos a contratar el de suministro de una plataforma de gestión centralizada para los dispositivos de seguridad (versión de máquina virtual) del mismo fabricante que los firewalls, que cumpla la función de plataforma integrada para la administración centralizada de los firewalls de seguridad propuestos.

Las características principales de la solución son:

- Permite crear una gestión delegada en modo multi-tenant.
- Incluye capacidades de control de acceso basada en permisos y gestión del cambio con aprobación.

- Incluye funciones de actualización de firmas de seguridad para permitir entornos "airgaped" en Firewalls internos.
- Dispone de conectores con cloud público (AWS, Azure, GCP, ACS, IBM Cloud, OCI) para obtener atributos de instancias y servicios y poder usarlos como objetos de reglas de firewall y políticas de SDWAN.
- Permite la gestión, aprovisión y administración de FWs, puntos de acceso, conmutadores y routers 4/5G en una sola plataforma.
- Permite el inventariado, ubicación y atributos HW, SW de todos los dispositivos conectados a la electrónica gestionada.
- Incluye una plantilla de aprovisionamiento utilizando código Jinja.
- Permitir agregar 10 dispositivos o dominios virtuales y manejar unos 2 GB de logs por día.

Además, incluye un **servicio de soporte avanzado** para un mínimo de 10 dispositivos o dominios virtuales (con soporte directo del fabricante) durante **dos años**.

5.1.6 Herramientas de control de acceso.

5.1.6.1 Herramienta de acceso privilegiado (PAM).

Se incluye dentro del alcance de los elementos a contratar una solución que centralice y automatice el control de las credenciales de administradores y usuarios externos con privilegios elevados, del mismo fabricante que los firewalls (Privileged Access Management (PAM)).

Las características principales de la solución son:

- Se instala en una única VM.
- Soporta controles ZTNA mediante la integración de la plataforma de acceso remoto VPN/ZTNA para el acceso a la plataforma y a los secretos.
- Incluye un licenciamiento basado en número de usuarios dados de alta en la plataforma, no en funcionalidades.
- Dispone tanto de tokens físicos como software además de FIDO2, si se requiriesen, para el mismo fabricante de la solución de PAM.
- Permite el uso de aplicaciones nativas del cliente, RDP, SSH, sin necesidad de instalar aplicaciones o plugins adicionales al agente ZTNA.
- Incluye soporte técnico avanzado.

La herramienta debe permitir **gestionar, como mínimo, 75 usuarios en una sola estación de trabajo virtual, durante 2 años**.

5.1.6.2 Herramienta para la gestión de acceso remoto VPN/ZTNA.

Se incluye dentro del alcance de los elementos a contratar una solución que ofrezca seguridad de acceso remoto y Zero Trust Network Access para 500 endpoints.

Las características principales de la solución son:

- Se integra de forma nativa con los firewalls para sincronización de telemetría y etiquetas ZTNA.
- Se integra de forma nativa con la herramienta de gestión de logs, eventos y reporting.

- Permite sincronizar de forma automática las políticas de webfilter del servidor de gestión centralizada para aunar las políticas de navegación a través de firewall y cuando el usuario se encuentra en remoto.
- Está alojada en un cloud privado del fabricante ubicado en Europa.
- Soporta SO, Windows, MAC OS, Linux, Android e IOS.
- Permite la gestión del enpoint, distribución de certificados, instalación, actualización y desinstalación del agente de forma remota.
- Realiza un inventario de aplicaciones instaladas y escaneo de vulnerabilidades con capacidades de remediación.
- Sirve el mismo cliente para la conexión contra la herramienta de acceso privilegiado.
- Incluye soporte técnico avanzado.

La herramienta debe permitir **gestionar, como mínimo, 500 endpoints durante 2 años**.

5.1.6.3 Herramienta de despliegue de honeypots.

Se incluye dentro del alcance de los elementos a contratar una herramienta de seguridad que implemente una estrategia de defensa mediante tácticas de engaño, del mismo fabricante que los firewalls.

Las características principales de la solución son:

- Se integrar de forma nativa con:
  - Firewalls para el aislamiento de dispositivos en caso de interacción con señuelo.
  - Directorio activo para la desactivación de una cuenta legitima detectada con uso fraudulento.
- Soporta un mínimo de 20 señuelos con las siguientes apariencias:
  - Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016, 2019 and 2022 (customizable BYOL), Linux (Ubuntu, CentOS, Redhat), macOS, SSL-VPN Server, Medical (PACS, Infusion pump), POS, ERP, IoT (Router, Switch, Printer and IPCamera), OT (PLC, HMI, MNG), SAP, SCADA, Outbreak,VOIP (4G/5G), TOMCAT, Webmin, Citrix, ESXi, Elastic-Search, SWIFT.
- Soporta como mínimo los siguientes servicios: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, SRTP, MOXA, KAMSTRUP, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP, TCP port listener, SMTP, RADIUS, Mysql, MQTT, SIP, XMPP, 3GPP, CANBus, B.BRAUN and VNC.
- Incluye servicios para dos VLAN's.
- Incluye soporte técnico avanzado.

La herramienta se debe suministrar durante **2 años** y debe soportar **servicio para Windows 7 y Windows 10**.

5.2 Servicios de instalación, configuración y puesta en marcha.

Quedan incluidos dentro del alcance de los servicios a prestar por el contratista la instalación, configuración y puesta en marcha de los equipos a suministrar en las instalaciones de la APB, de acuerdo con sus especificaciones.

Durante el arranque del contrato, la APB se reunirá con la empresa adjudicataria con el objeto de ajustar dicho plan a los requerimientos de la APB, en caso de que sea necesario.

El servicio de instalación configuración y puesta en marcha comprende la realización de las siguientes actuaciones:

- Instalación física de los elementos en los CPDs (según puerto) y del cableado intra-rack que conecte entre si los diferentes elementos y conexión con el resto de la infraestructura de APB.
- Retirada y reciclaje de los embalajes.
- Configuración de la solución para su puesta en marcha siguiendo la recomendación de buenas prácticas aportadas por el fabricante.
- Para hacer la puesta en marcha con la mínima afectación al servicio posible, el adjudicatario configurará los firewalls en modo transparente y tendrá que auditar durante un período aproximado de 5 días el tráfico saliente, generando una propuesta de configuración que será validada y contrastada por la APB. Una vez consensuada la lista se aplicará la configuración y, con el adjudicatario se podrá in situ, si es necesario, hacer los cambios de manera urgente que fueran necesario aplicar.
- Pruebas del correcto funcionamiento de todos los equipos instalados.
    - Inicialmente se realizará una prueba PILOTO con una sede, una vez que se haya comprobado toda la instalación, se desplegarán el resto de sedes con el mismo estándar que la sede piloto exceptuando las particularidades propias de cada sede, que deberán ser integradas en cada SEDE.
    - Se deberán realizar las reuniones de seguimiento necesarias con la APB para el correcto seguimiento del proyecto (en la sede de la APB o de forma remota).
    - La configuración deberá tener en cuenta los siguientes datos de la APB:
        - Arquitectura de RED.
        - Configuración VLAN's APB.
        - Configuración DHCP Direccionamiento APB.
        - Configuración SDWAN para futura implantación.
        - Coordinación con el operador para el enrutamiento de las delegaciones hacia la central de la APB.
        - Seguir las directrices de la APB para la implantación de la solución.
        - Coordinación en la ejecución del proyecto con la APB.

La empresa adjudicataria **deberá tener en cuenta que se debe compatibilizar la instalación y configuración de los** dispositivos con la operativa habitual de los puertos de Palma, Alcudia, Maó, Eivissa y La Savina. Por tanto, la empresa adjudicataria deberá tener en cuenta en su oferta que cabe la posibilidad que no todos los trabajos se podrán realizar en días consecutivos, horario diurno o en horario laboral. Así, deberá adaptar los trabajos a las franjas de horarios más adecuadas para la APB, pudiendo ser fines de semana o fuera del horario laboral.

5.3 Servicios de formación.

Para una implantación exitosa de esta contratación, es necesario llevar a cabo actuaciones orientadas a la formación del personal de la APB.

El servicio incluye un completo plan de formación a los técnicos en los equipos y las herramientas implantadas para la operación de los mismos, consulta y seguimiento de seguridad, obtención de informes y métricas de funcionamiento, etc. La estimación definitiva del número de sesiones formativas, su duración, contenidos, número y perfil de los asistentes,

así como aquellos aspectos no especificados, se determinarán en base a las necesidades detectadas por la APB.

Esta formación deberá ser impartida on-line, con la plataforma de la APB, por personal certificado en la solución ofertada. Todas las sesiones de formación serán grabadas por la APB para ponerlas a disposición de su personal.

Los técnicos del adjudicatario encargados de llevar a cabo la formación deberán tener la certificación del fabricante.

Como norma general, todas las sesiones de formación incluirán la entrega de documentación al inicio de las mismas para todos los participantes. Previamente a la impartición de las formaciones, el Responsable del Contrato deberá haber aprobado el contenido de las mismas, que deberá ser modificado/adaptado por la empresa adjudicataria, sin coste adicional para la APB.

5.4 Servicios de soporte técnico y consultoría.

El servicio de soporte incluye la prestación de un servicio remoto de soporte técnico y consultoría para consultas, así como para la inclusión de nuevas funcionalidades. Este servicio se prestará a través de la definición de una bolsa de 100 horas de consultor.

Este servicio, que debe permitir escalar cualquier consulta sobre las soluciones ofertadas por la empresa adjudicataria, se llevará a cabo de acuerdo a las siguientes especificaciones:

- La empresa adjudicataria deberá establecer un número de teléfono de soporte sin coste adicional asociado a la llamada (que no sea un teléfono tipo 902 o similar), con un horario mínimo de lunes a viernes de 9:00 a 18:00 para dar soporte a los usuarios de la APB que lo requieran, atendiendo incidencias de cualquier tipo relacionadas con el servicio.
- La empresa adjudicataria realizará una valoración detallada de las tareas a realizar, en referencia a nuevas funcionalidades a implantar, para completar los trabajos solicitados y cuantificará cada tarea en horas de cada perfil, así como el tiempo de ejecución de los mismos.
- Si el Responsable del Contrato de la APB aprueba la valoración de los trabajos la empresa adjudicataria realizará la tarea. En caso de no aprobar los trabajos no se descontará ninguna hora. No se descontará ninguna hora a la bolsa, si previamente no ha sido aprobado por el Responsable del Contrato de la APB.
- Una vez terminados los trabajos y aceptados por parte del Responsable del Contrato de la APB se descontarán las horas aprobadas de la bolsa de horas. Sin el cumplimiento de estos requisitos los trabajos no serán facturables.
- La horas incluidas en esta bolsa de horas correspondiente a este servicio serán opcionales (es decir, no es obligatorio para la APB consumir el total de las horas incluidas en esta bolsa) y no caducarán a lo largo de la vigencia del contrato, siendo solo facturadas las horas realmente efectuadas.
- Los técnicos designados por el adjudicatario para llevar a cabo este servicio de soporte y consultoría deberán estar certificados por el fabricante para poder realizar estos trabajos.

6 Entregables

Como resultado de los trabajos realizados, la empresa adjudicataria deberá entregar como mínimo la documentación indicada en este apartado.

La documentación generada durante la ejecución del contrato será de propiedad exclusiva de la APB sin que la empresa adjudicataria pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de la APB, que la daría en su caso previa petición formal de la empresa adjudicataria con expresión del fin.

El coste de elaboración y/o actualización de la documentación generada en el contrato, está incluida en las partidas correspondientes de cada una de las actuaciones.

La documentación se entregará en formato editable (LibreOffice o Microsoft Office) y en formato pdf.

1. Sistema de protección perimetral:
   - i. Licencias correspondientes a los soportes y servicios incluidos. Se debe aportar el documento que acredite la contratación del servicio con el fabricante, con la modalidad de soporte y mantenimiento contratada y las fechas en las que va a ser efectivo, así como el licenciamiento asociado.
   - ii. Informes mensuales relativos a las actuaciones de soporte y de servicio realizadas y los resultados obtenidos, relativos a los servicios de seguridad ofrecidos y a las herramientas de gestión de los NGFW, así como las recomendaciones de acciones a realizar, si las hubiera.
2. Servicios de instalación, configuración y puesta en marcha:
   - iii. Plan de proyecto.
   - iv. Definición de la configuración del suministro.
   - v. Definición de la integración en la red de la APB.
   - vi. Plan de pruebas de la operatividad del sistema.
   - vii. Actas de entrega de los suministros.
3. Servicios de formación:
   - viii. Plan de formación.
   - ix. Informes de seguimiento del plan de formación.
   - x. Informes de formación de usuario final.
   - xi. Documentación utilizada en la formación.
4. Servicios de soporte técnico y consultoría:
   - xii. Informes mensuales relativos a las actuaciones de soporte técnico realizadas y resultados obtenidos.
   - xiii. Documentos de las peticiones de consumo de la bolsa de horas y presupuestos.

7 Acuerdos de nivel de servicio y penalizaciones

7.1 Acuerdos de nivel de servicio

La prestación de los servicios objeto de este Pliego estarán sujetos a acuerdos de nivel de servicio (ANS) con penalizaciones asociadas en caso de incumplimiento. La finalidad de los ANS es establecer un marco objetivo para medir el cumplimiento de los compromisos adquiridos en el contrato.

Se definirán ANS que establecerán los umbrales mínimos de calidad exigidos en la prestación de los servicios definidos en el apartado 5 de este Pliego. En su caso, se aplicarán los ANS

propuestos por la empresa adjudicataria en su oferta técnica y aceptados por el Responsable del Contrato.

7.1.1 ANS de puesta en marcha de los equipos, soportes y servicios.

El incumplimiento por parte de la empresa adjudicataria del plazo máximo de puesta en marcha de los equipos suministrados, por motivo ajenos a la APB, incurrirá en la siguiente penalización:

Código	Cálculo	Valor Objetivo
RESP01	Desviación en días desde el plazo máximo de puesta suministro, instalación, configuración y testeo del sistema de protección perimetral	10 días laborables
RESP02	Desviación en días desde la puesta en marcha de los soportes y servicios a ofrecer, así como de las herramientas de gestión de los NGFW	10 días laborables
RESP03	RESP03 = Total incidencias prioridad crítica respondidas en plazo * 100 / Total incidencias prioridad critica	90%
RESP04	RESP04 = Total incidencias prioridad no crítica respondidas en plazo * 100 / Total incidencias prioridad no critica	80%

En cuanto a la clasificación de las incidencias, se definen las siguientes:

- **Incidencia crítica.** Se considerará una incidencia crítica aquella que suponga un problema grave que afecte significativamente a las operaciones normales de un sistema o red y que suponga una interrupción total o una disminución significativa de la calidad de un servicio esencial.
- **Incidencia no crítica.** Se considerará como una incidencia no crítica, aquella que no tiene un impacto significativo en las operaciones normales de un sistema o red, tales como problemas menores, errores no críticos, o cuestiones que no afectan la funcionalidad principal o la disponibilidad del sistema.

7.1.2 ANS de gestión de la documentación

La prestación de los servicios descritos en el apartado 5 de este Pliego vendrá acompañada de la documentación correspondiente y definida por los estándares de aplicación (UNE-ISO/IEC 20000 -ITIL o la propuesta por la empresa adjudicataria), así como la exigida en el apartado 6 de este Pliego. Se establecen los siguientes indicadores:

1. **Auditoría de calidad de la documentación.** Control de la actualización o existencia de documentación mediante auditorías del servicio que realice la APB.

Código	Cálculo	Valor Objetivo

DOCU01	Control de la documentación = (Número de documentos no actualizados o inexistentes, detectados / Número de documentos auditados) x 100	100 %

2. **Entrega fuera de plazo de la documentación.** Comprobación de que la documentación ha sido presentada en los plazos previstos. Este indicador se aplicará a cualquier otra documentación que, como consecuencia de la ejecución del contrato, pudiera solicitarse y para el que se hubiere acordado un plazo de presentación.

Código	Cálculo	Valor Objetivo
DOCU02	Número de documentos entregados fuera de plazo	0 días

7.1.3 Penalizaciones

Los ANS del apartado anterior fijan los niveles de servicio mínimos que se consideran adecuados para desempeñar la prestación de los servicios objeto de este Pliego. Con carácter mensual, se calcularán todos los indicadores para medir si han existido desviaciones sobre los niveles de referencia.

Aquellos niveles de servicio que estén por debajo de los umbrales marcados por los indicadores, estarán sujetos a las penalizaciones indicadas en el Cuadro de Características del Pliego Administrativo.

8 Garantía

Se fija un periodo de garantía de 3 años desde la fecha de la correspondiente acta de recepción para todos los elementos suministrados.

La garantía deberá incluir el licenciamiento de todos los sistemas suministrados, así como el soporte técnico por parte de los fabricantes, cubriendo las incidencias en cualquier componente que suponga un funcionamiento deficiente atendiendo a los requisitos establecidos en el presente pliego de prescripciones técnicas, así como las actualizaciones de versiones o parches de los elementos objeto del contrato que sean susceptibles de ello.

Durante el plazo de garantía deberán realizarse todos los trabajos necesarios para la reparación o reposición de cualquier elemento de los sistemas suministrados.

Ello sin menoscabo de ampliar la responsabilidad de la empresa adjudicataria para las actuaciones, contenidas o no en el alcance definido en el presente documento, manifiestamente incompletas, incorrectas o deficientes, siempre que sean imputables a la empresa adjudicataria.

9 Plazo y lugar de ejecución

El plazo total de ejecución del contrato se establece en **un máximo de 27 MESES** desde el inicio de los trabajos (Acta de Inicio).

Se establece un primer **plazo parcial máximo de TRES MESES** para el suministro, instalación, configuración y testeo del sistema de protección perimetral, contados a partir de la firma del Acta de Inicio.

Se establece un segundo **plazo parcial máximo de VEINTICUATRO (24) MESES**, contados a partir de la firma del Acta de Recepción del suministro, instalación, configuración y testeo del sistema de protección perimetral, para las licencias/suscripciones a los soportes y servicios anuales del sistema de protección perimetral de red, incluidos en esta contratación, de acuerdo con el calendario indicado en este apartado.

El calendario previsto para la realización del servicio durante el plazo de vigencia inicial se desarrollará teniendo en cuenta las tareas que se identifican en el apartado 5 de este Pliego.

Suministros y servicios	AÑO 1		AÑO 2				AÑO 3		
	T3	T4	T1	T2	T3	T4	T1	T2	T3
Suministro, instalación, configuración y puesta en marcha del sistema de protección perimetral									
Soporte y servicios referidos a los sistemas de protección perimetral									
Formación									
Soporte técnico y consultoría									
Gestión del proyecto									

Periódicamente y a requerimiento de la APB la empresa adjudicataria deberá informar de la situación en la que se encuentra el proyecto, de acuerdo con la planificación indicada.

Los suministros y los servicios de instalación, configuración y puesta en marcha se llevarán a cabo según lo dispuesto en el presente pliego, teniendo en cuenta las distintas sedes (Palma, Maó, Eivissa, Alcúdia y La Savina) donde deben ser realizados dichos suministros y servicios.

El resto de los servicios se llevarán a cabo según se especifica en este pliego de prescripciones técnicas. En caso necesario, la APB podrá autorizar la presencia de personal de la empresa adjudicataria en las oficinas de la APB sitas en Moll Vell nº5 de Palma de Mallorca, para las reuniones y actividades propias para el desarrollo de los trabajos objeto del presente Pliego.

10 Medios humanos mínimos

La empresa adjudicataria deberá designar a un responsable o jefe de proyecto que actuará como interlocutor ante la APB, y que realizará las tareas de dirección, planificación y coordinación de los trabajos.

El equipo humano propuesto para la ejecución de los trabajos de esta licitación deberá contar con las certificaciones adecuadas, en referencia a:

- La certificación del fabricante de los técnicos encargados de la configuración de la solución para su puesta en marcha.
- La certificación del fabricante para el técnico o técnicos encargados de realizar la formación solicitada.

El equipo humano propuesto se incorporará tras la formalización del contrato para la ejecución de los trabajos.

La falsedad en el nivel de conocimientos técnicos de los perfiles que se incorporen, deducida del contraste entre la información especificada en la oferta y los conocimientos reales demostrados en la ejecución de los trabajos, implicará la no facturación de los trabajos realizados en estas condiciones y la sustitución del mismo y, en su caso, la resolución del contrato.

11 Certificaciones de la empresa adjudicataria

La empresa adjudicataria deberá tener vigentes las siguientes certificaciones:

- Certificación ISO 9001 – Sistema de gestión de calidad.
- Certificación ISO -14001 – Sistema de gestión medioambiental.
- Certificación ISO -27001 – Sistema de Gestión de Seguridad de la Información.
- Certificación del Esquema Nacional de Seguridad (ENS) Nivel MEDIO.

Deberá disponer además de un certificado actualizado y firmado por el fabricante de los equipos y soportes ofertados, que acredite la relación que la empresa mantiene con el mismo, y que garantice el suministro de las actualizaciones, parches y correcciones de microcódigo, programas de diagnóstico, manuales actualizados, y apoyo técnico experto de los ingenieros de producto en caso necesario.

12 Presupuesto, recepción de los trabajos y forma de pago

12.1 Presupuesto máximo de licitación

El **presupuesto base de licitación** correspondiente a las dos anualidades del contrato (incluido en el Anexo IV. Presupuesto) asciende a la cantidad de **SETECIENTOS VEINTICUATRO MIL QUINIENTOS SESENTA EUROS CON CINCUENTA Y SEIS CÉNTIMOS (724.560,56)** de los que **CIENTO VEINTICINCO MIL SETECIENTOS CINCUENTA EUROS CON DIECIOCHO CÉNTIMOS (125.750,18)** corresponden al 21% de IVA y **QUINIENTOS TRES MIL DOSCIENTOS DOS EUROS (503.202,00)** al presupuesto de inversión.

A efectos de justificación de precios, en el anexo correspondiente (Anexo III. Justificación de precios), se tiene en cuenta los artículos 100 y 102 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

Están incluidos en los precios anteriores todos los costes derivados de la ejecución material de los servicios, los gastos generales de estructura y el beneficio industrial. Además, dichos precios se ajustan a los precios de mercado para los equipos, soportes y servicios incluidos e incluyen todos los costes laborales, ajustándose al Convenio Colectivo vigente.

La recepción de los trabajos será parcialmente para cada uno de ellos, hasta que se hayan completado el total de los que se prevén en este contrato. Se podrán realizar actas de recepción parcial de los trabajos, recogiendo los entregables de la etapa recibida.

Los gastos de desplazamientos y dietas y otros costes complementarios por los distintos viajes y servicios que deberá realizar el personal de la empresa adjudicataria para la ejecución de los trabajos, así como el alquiler o amortización de oficinas o locales y demás bienes que sean necesarios para el desarrollo de los mismos, así como seguros, tributos, gravámenes, tasas y cualquier otro gasto necesario para llevar a cabo los servicios objeto del Contrato, no supondrán ningún incremento de coste.

12.2 Medición y abono de los trabajos

La unidad de medición de los trabajos será la indicada en la descripción de la partida económica. En caso de omisión o contradicción entre documentos o partes de documentos, será la indicada por el Responsable del Contrato.

Para el abono de los trabajos, sólo se admitirán los precios unitarios del presente Pliego, a los que se les aplicará el coeficiente de adjudicación resultante (cociente entre el importe ofertado y el de licitación).

El abono se realizará por unidad realmente ejecutada, siempre que exista conformidad por parte del Responsable del Contrato o en quien delegue. El importe a resarcir se obtendrá de la multiplicación de la medición los trabajos ejecutados por el precio unitario de dicho trabajo afectado por el coeficiente de adjudicación (cociente entre el importe ofertado y el de licitación).

Para ello se elaborará el documento "Relación valorada" que contendrá la relación de trabajos ejecutados, el precio unitario y el coeficiente de adjudicación a aplicar.

Dicha "Relación valorada" deberá ser **firmada electrónicamente** de conformidad, como mínimo por el representante de la empresa adjudicataria y por el Responsable del Contrato. Su cumplimentación será indispensable para el abono de los trabajos realizados.

El Responsable del Contrato elaborará el documento "Certificación" a partir de la información recogida en la "Relación valorada" y hará llegar al representante de la empresa adjudicataria el **ID de certificación asignado**.

12.3 Forma de pago

Una vez facilitado el número ID de certificación (nunca antes), la empresa adjudicataria podrá proceder a la emisión de la factura y su posterior remisión a la APB vía FACe.

Para que la factura sea válida deberá consignarse en el envío FACe:

- ID de certificación asignado.
- Datos identificativos del expediente.
- Importe de facturación, que deberá ser coincidente al segundo decimal con el de la "Relación valorada".

13 Seguridad

13.1 Acceso a los sistemas de la APB

En caso de que el personal de la empresa adjudicataria necesite conectarse a los sistemas de información de la APB, ya sea local o remotamente, la empresa adjudicataria deberá identificar

a todos y cada uno de sus empleados que vayan a realizar el mencionado tipo de actividades, con el fin de asignarles a cada uno de ellos credenciales de acceso personalizadas.

La empresa adjudicataria se obliga a transmitir al personal mencionado anteriormente la necesidad de custodiar diligentemente sus credenciales, evitando compartirlas o revelarlas. En caso de que las credenciales sean reveladas, la empresa adjudicataria deberá comunicar tal circunstancia de forma inmediata a la APB para que sean revocadas.

En caso de que algún empleado con acceso a los sistemas de la APB causara baja, la empresa adjudicataria deberá poner en conocimiento de la APB tal circunstancia de forma inmediata.

13.2 Cambios

Cualquier cambio que la empresa adjudicataria vaya a realizar en sus procesos, sus infraestructuras y, en general, en su entorno, y que pudiera afectar directa o indirectamente a la APB o al objeto del contrato, debe ser previamente comunicado y consensuado con la misma.

13.3 Incidentes de seguridad de la información

La empresa adjudicataria deberá comunicar de inmediato a la APB cualquier incidente de seguridad de la información que hubiera afectado al entorno de la empresa adjudicataria (malware, fugas de información, etc.) que pudiera afectar, a su vez, a la APB, ya sea a través de correos electrónicos, pendrives, equipos portátiles, el propio personal o por cualquier otro medio.

13.4 Derecho de auditoría

La empresa adjudicataria deberá admitir, y facilitará a la APB, la realización de auditorías que permitan comprobar que la empresa adjudicataria cumple con los requisitos de seguridad establecidos en el marco del contrato.

13.5 Subcontratación

En caso de que se subcontrate alguno de los servicios incluidos en el presente proyecto, la empresa adjudicataria deberá transmitir a los posibles subcontratistas todos los requisitos establecidos en los pliegos de condiciones administrativas y técnicas, y muy especialmente, aquellos requisitos relacionados con la disponibilidad, integridad y confidencialidad de la información y de los servicios de la APB.

13.6 Servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la APB

La empresa adjudicataria deberá disponer de la suficiente redundancia en sus infraestructuras como para ofrecer un servicio con garantías de disponibilidad a la APB.

La empresa adjudicataria deberá disponer de un plan de continuidad de su negocio o un plan de recuperación de desastres que afecten a sus infraestructuras relacionadas con el objeto del contrato. Estos planes estarán a disposición de la APB para ser revisados en caso de que se estimara oportuno por parte de la APB.

13.7 Otros

Se valorará que la empresa adjudicataria utilice sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

14 Defectos o deficiencias de los trabajos

Todos los trabajos desarrollados por el contratista deberán ser aceptados por la APB, antes de considerarse entregados a efectos de responsabilidad del contratista.

En el caso de que el Responsable del Contrato presentara reparos para la aceptación de los trabajos debidamente comunicados a la empresa adjudicataria, y éstos se derivaren de errores, incumplimientos de normas o reglamentos técnicos; o bien errores de cualquier aspecto de los trabajos cuya realización haya incumbido a la empresa adjudicataria, será obligación de ésta subsanar las deficiencias en los términos que se señalen por el Responsable del Contrato, y en los plazos que éste conceda, sin que por ello tenga derecho a compensación económica alguna.

La posibilidad de apreciación de defectos por la APB con responsabilidad del adjudicatario no expira hasta transcurrido el periodo de garantía del contrato.

15 Contradicciones y omisiones del presente documento

Las omisiones erróneas de los detalles que sean indispensables para llevar a cabo los trabajos descritos según el espíritu e intención expuestos en estas prescripciones técnicas, o que, por uso y costumbre deban ser realizados, no sólo no eximen a la empresa adjudicataria de la obligación de ejecutar estos detalles omitidos o erróneamente descritos, sino que, por el contrario, deberán ser ejecutados como si hubieran sido completos y correctamente especificados en este Documento.

16 Consideración final

Las condiciones del presente Documento prevalecen, en lo que pudiera ocurrir de oposición, sobre cualesquiera otros de carácter técnico o administrativo que pudiera tener establecidos el adjudicatario para la prestación de servicios a personas físicas o jurídicas privadas, siendo en todo caso de aplicación al Contrato cuanto previene la normativa vigente.

El desconocimiento del Contrato o de cualquiera de sus términos, de los documentos anexos que forman parte del mismo, o de las instrucciones, pliegos o normas de toda índole aprobadas por la Administración que puedan ser de aplicación en la ejecución de los servicios objeto del Contrato, no eximirá al adjudicatario de la obligación de su cumplimiento.

Palma, a fecha de firma del documento

Autor del Documento	Revisado y Conforme
José Miguel Esteve Lledó	***Javier Segovia Mascaró***
Responsable de Sistemas de Información e Infraestructuras TIC	Jefe del Departamento de Desarrollo Tecnológico e Innovación

Aprobación

Antonio Ginard López

Director

Anexo I. Ficha de perfil profesional

Datos del perfil (1 hoja por perfil aplicable al objeto del contrato):

Identificación oferta:	
Empresa licitadora:	
Perfil:	
Nombre y apellidos:	

	Requisitos mínimos			
Certificación del fabricante:	(Sí/No)			
Código	Certificación	Horas	Entidad/Organismo	F-inicio
F1				
…				
Fn				

Se ha de especificar si se cumplen o no los requisitos mínimos exigidos en el Pliego.

Titulación (MECES):	(Sí/No)	T1, T2, …, Tn
Experiencia (años):	(Años)	P1, P2, …, Pn
Dedicación (%)	% mínimo	
Formación específica/complementaria:	(Sí/No)	F1, F2, …, Fn

Titulación académica, Formación y Datos relativos a los proyectos en los que ha participado relacionados con las funciones a realizar en el contrato para acreditar los diferentes aspectos.

Currículo profesional:

Empresa	Categoría	F-alta	F-baja	Meses	Actividad realizada

Formación – otras certificaciones relacionadas con el objeto del expediente:

Código	Curso/Certificación	Horas	Entidad/Organismo	F-inicio

F1				
…				
Fn				

Titulación académica[1]:

Código	Título académico	Centro	Años	F-expedición	Objeto Expediente
T1					
…					
Tn					

Años: duración oficial.

Objeto expediente: Sí/No según sea requisitos para el contrato o no.

Datos relativos a los proyectos en los que ha participado relacionados con las funciones a realizar en el contrato:

Código	Proyecto	Perfil	F-inicio	F-fin	Entidad usuaria	Descripción
P1						
…						
Pn						

Perfil: El ejercido en el proyecto.

Nota: Todas las fechas deberán consignarse en el formato dd/mm/aaaa.

[1] La titulación deberá ser oficial, o en su defecto, reconocida por el Ministerio de Educación y Formación Profesional.

Anexo II. Solvencia técnica de la empresa

Relación de proyectos similares realizados

Identificación oferta:	
Empresa licitadora:	

Nº Orden	Nombre Proyecto	Organismo/Empresa contratante	Fecha	Plazo	Importe licitación	Descripción
P1						
…						
Pn						

Perfil	Nº de empleados

Anexo III. Justificación de precios

Los costes unitarios salariales incluidos en esta contratación se han estimado a partir del convenio laboral de referencia "*Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública*" y son los siguientes (sin IVA):

PERFILES	**Precio/hora**
Consultor Senior	52,42 €
Consultor	42,02 €

A estos costes se debe añadir los correspondientes porcentajes correspondientes a:

- Beneficio Industrial (BI): 6%
- Gastos Generales (GG): 13%

Así mismo, se incluye a continuación el desglose de los servicios referidos a la instalación, configuración y puesta en marcha, así como los servicios de formación, soporte técnico y consultoría. Los costos en referencia a la dirección, planificación y coordinación de los trabajos están incluidos en las partidas de los servicios correspondientes.

CAP.6		**INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA**	**Cantidad**	**Importe**	**Total**
6.1	Ud	Instalación, configuración y puesta en marcha, según especificaciones PPT	1,00	30.800,00 €	30.800,00 €
	h	Consultor Senior	330,00	52,42 €	17.298,00 €
	h	Consultor	266,30	42,02 €	11.189,00 €
	%	Medios auxiliares (2%)	28.487,00 €	0,02	570,00 €
	%	Costes Indirectos (6%)	29.057,00 €	0,06	1.743,00 €
CAP.7		**SERVICIOS DE FORMACIÓN**	**Cantidad**	**Importe**	**Total**
7.1	Ud	Formación, según especificaciones PPT	1,00	1.500,00 €	1.500,00 €
	h	Consultor	33,00	42,02 €	1.387,00 €
	%	Medios auxiliares (2%)	1.387,00 €	0,02	28,00 €
	%	Costes Indirectos (6%)	1.415,00 €	0,06	85,00 €
CAP.8		**SERVICIOS DE SOPORTE TÉCNICO Y CONSULTORÍA**	**Cantidad**	**Importe**	**Total**
8.1	h	Bolsa de horas, según especificaciones PPT	100,00	42,02 €	4.202,00 €
	h	Consultor	100,00	42,02 €	4.202,00 €

Nota: Para facilitar la simplificación de los cálculos, alguno de los totales se ha redondeado.

Anexo IV. Presupuesto.

Presupuesto					
Adquisición de equipos físicos y servicios de ciberseguridad perimetral para la Autoridad Portuaria de Baleares					
CAP.1		**EQUIPOS (NGFW)**	**Cantidad**	**Importe**	**Total**
1.1	Ud	Equipo tipo A (Palma)	4,00	22.000,00 €	88.000,00 €
1.2	Ud	Equipo tipo B (Maó, Eivissa)	4,00	9.600,00 €	38.400,00 €
1.3	Ud	Equipo tipo C (Alcúdia, La Savina)	4,00	1.300,00 €	5.200,00 €
CAP.2		**SOPORTES DE SEGURIDAD PARA LOS EQUIPOS**	**Cantidad**	**Importe**	**Total**
2.1	Ud	Soporte de seguridad avanzado para Equipo tipo A (anual)	8,00	17.800,00 €	142.400,00 €
2.2	Ud	Soporte de seguridad avanzado para Equipo tipo B (anual)	8,00	6.700,00 €	53.600,00 €
2.3	Ud	Soporte de seguridad avanzado para Equipo tipo C (anual)	8,00	1.100,00 €	8.800,00 €
2.4	Ud	Soporte de seguridad avanzado para entornos de OT Equipo tipo A (anual)	8,00	5.100,00 €	40.800,00 €
2.5	Ud	Soporte de seguridad avanzado para entornos de OT Equipo tipo B (anual)	8,00	2.100,00 €	16.800,00 €
2.6	Ud	Soporte de seguridad avanzado para entornos de OT Equipo tipo C (anual)	8,00	300,00 €	2.400,00 €
CAP.3		**HERRAMIENTAS DE MONITORIZACIÓN Y GESTIÓN DE LOS NGFW**	**Cantidad**	**Importe**	**Total**
3.1	Ud	Herramienta de gestión de registros	1,00	4.200,00 €	4.200,00 €
3.2	Ud	Orquestador de Firewalls que permita agregar un mínimo de 10 dispositivos o dominios virtuales	1,00	700,00 €	700,00 €
CAP.4		**SERVICIOS Y SOPORTES PARA LAS HERRAMIENTAS DE MONITORIZACIÓN Y GESTIÓN**	**Cantidad**	**Importe**	**Total**
4.1	Ud	Soporte avanzado para la herramienta de gestión de registros (mínimo 26GB/día de logs) (anual)	2,00	1.400,00 €	2.800,00 €
4.2	Ud	Servicio de automatización de seguridad para la herramienta de gestión de registros (mínimo 26GB/día de logs) (anual)	2,00	3.500,00 €	7.000,00 €
4.3	Ud	Servicio de detección de IOC y brotes para la herramienta de gestión de registros (mínimo 26 GB/día de logs) (anual)	2,00	1.700,00 €	3.400,00 €
4.4	Ud	Soporte avanzado para el orquestador de firewalls (mínimo 10 dispositivos o dominios virtuales) (anual)	2,00	300,00 €	600,00 €
CAP.5		**HERRAMIENTAS DE CONTROL DE ACCESO**	**Cantidad**	**Importe**	**Total**
5.1	Ud	Herramienta de acceso privilegiado PAM para un mínimo de 75 usuarios incluyendo soporte avanzado (anual)	2,00	18.300,00 €	36.600,00 €

5.2	Ud	Herramienta para la gestión de acceso remoto VPN/ZTNA para un mínimo 500 endpoints incluyendo soporte avanzado (anual)	2,00	3.500,00 €	7.000,00 €
5.3	Ud	Herramienta de despliegue de honeypot (mínimo de 2 VLAN's) (anual)	2,00	2.100,00 €	4.200,00 €
5.4	Ud	Soporte para Windows 7 y Windows 10 de la herramienta de despliegue de honeypot (2 años)	1,00	3.800,00 €	3.800,00 €
CAP.6		**INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA**			
6.1	Ud	Instalación, configuración y puesta en marcha, según especificaciones PPT	1,00	30.800,00 €	30.800,00 €
CAP.7		**SERVICIOS DE FORMACIÓN**			
7.1	Ud	Formación, según especificaciones PPT	1,00	1.500,00 €	1.500,00 €
CAP.8		**SERVICIOS DE SOPORTE TÉCNICO Y CONSULTORÍA**			
8.1	h	Bolsa de horas, según especificaciones PPT	100,00	42,02 €	4.202,00 €
				PRESUPUESTO BASE DE LICITACIÓN (2 AÑOS)	**503.202,00 €**
				Beneficio Industrial (6%)	30.192,12 €
				Gastos Generales (13%)	65.416,26 €
				PRESUPUESTO BASE DE LICITACIÓN BI Y GG SIN IVA (2 AÑOS)	**598.810,38 €**
				IVA (21%)	125.750,18 €
				PRESUPUESTO BASE DE LICITACIÓN CON IVA (2 AÑOS)	**724.560,56 €**