E21-0107

ESPECIFICACIONES TÉCNICAS Y VALORACIÓN PARA LA CONTRATACIÓN DE

"HERRAMIENTA DE MONITORIZACIÓN DE LA RED INFORMÁTICA PARA LA AUTORIDAD PORTUARIA DE BALEARES"

ÍNDICE

1. ANTECEDENTES Y JUSTIFICACIÓN 1
2. OBJETO DEL PRESENTE DOCUMENTO 1
3. DESCRIPCIÓN DE LA SOLUCIÓN, REQUERIMIENTOS Y ESPECIFICACIONES DE LOS SERVICIOS 1
4. PLAZO PARA LA EJECUCIÓN DEL CONTRATO 6
5. PRESUPUESTO 6
6. PLAZO DE GARANTÍA 8
7. PRESCRIPCIONES TÉCNICAS GENERALES 8
8. CONDICIONES GENERALES 9
   8.1. MEDIDAS DE SEGURIDAD 9
   8.2. GASTOS DE CARÁCTER GENERAL A CARGO DEL CONTRATISTA 9
   8.3. MEDICIÓN Y ABONO DE LOS TRABAJOS 9
   8.4. CONTRADICCIONES Y OMISIONES DEL PRESENTE DOCUMENTO 10
   8.5. CONSIDERACIÓN FINAL 10

1. ANTECEDENTES Y JUSTIFICACIÓN

La sociedad actual se ha vuelto muy dependiente de las Tecnologías de la Información y Comunicaciones, las empresas, industrias y administraciones públicas realizan un uso masivo de las mismas. A la vez que se incrementa el uso de estas tecnologías, también se ha incrementado el riesgo de interrupción económica, social y física debido a las vulnerabilidades que estas tecnologías intrínsecamente poseen.

Estas vulnerabilidades son el origen de las incidencias provocadas por diferentes tipos de actores. Actualmente, el número de incidencias es alto y la complejidad grande para identificar las nuevas amenazadas y vulnerabilidades que presentan el mayor riesgo. Además, hay que reforzar las defensas y controles tradicionales para detectar nuevas tácticas y técnicas en las nuevas incidencias, que ahora pueden mezclarse en la inmensidad de la red y atravesar grandes y complejas infraestructuras en cuestión de segundos.

La Autoridad Portuaria de Baleares (en adelante, APB), gestiona cinco puertos de interés general, y como tales, sirven a industrias y establecimientos de importancia para la economía nacional y en particular de la Balear. Por todo ello, resulta esencial que la APB disponga de los medios tecnológicos para una protección de sus infraestructuras, información y los servicios ofrecidos.

2. OBJETO DEL PRESENTE DOCUMENTO

El objeto del presente Pliego es la contratación de un servicio que ofrezca una herramienta de análisis de red y respuesta aplicado a la seguridad para la APB, además de la contratación de servicios adicionales de monitorización continua de la red, análisis y soporte por expertos en el caso de detección de incidencias para los sistemas de la APB.

3. DESCRIPCIÓN DE LA SOLUCIÓN, REQUERIMIENTOS Y ESPECIFICACIONES DE LOS SERVICIOS

A continuación, se describen los criterios generales a cumplir por la herramienta a contratar, trabajos a realizar, así como las especificaciones técnicas del servicio requerido.

3.1. CRITERIOS DE LA SOLUCIÓN

La solución a implantar deberá cumplir los siguientes requisitos:

- Se trata de contratar una herramienta que abarque toda la infraestructura de red de los cinco puertos gestionados por la APB
- Solución escalable
- Solución basa da en inteligencia artificial (IA) de autoaprendizaje continuo.
- Capacidad de detección, alerta temprana y respuesta autónoma en tiempo real
- Investigación automatizada basa da en IA

- Servicios adicionales a proveer:
    - Servicio de soporte y apoyo continuo estándar
    - Servicio de soporte por expertos 24/7
    - Servicio 24/7 de monitorización y notificación proactiva de amenazas
    - Servicio de mantenimiento completo de todo el hardware
    - Actualizaciones continuas del software
    - Servicio de monitorización y notificación proactiva de amenazas 24/7
    - Implementación de aplicación móvil para administradores de la red con envío de alertas

3.2. TRABAJOS Y SERVICIOS INCLUIDOS

A continuación se indican los servicios y trabajos incluidos en el objeto del presente Pliego:

a) Instalación de una herramienta avanzada con las características descritas en el punto *3.3. Descripción de las características de los módulos de la solución*, en todos los puertos gestionados por la APB (Palma, Alcúdia, Maó, Eivissa y La Savina). Esta herramienta comportará un despliegue hardware de al menos:

- 1 Medium Appliance para la sede principal (Palma), en el CPD.
- 2 Small Appliances para sedes de Maó y de Eivissa
- 20 Client Sensors para los usuarios de las sedes de Alcudia y La Savina (Formentera)

b) La herramienta dispondrá al menos de las siguientes licencias software:

a. Módulo de detección de red: Licencia de Enterprise Immune System de Darktrace o equivalente para una red de 1.500 IPs máximas.
b. Módulo de respuesta autónoma: Licencia Antígena Network de Darktrace o equivalente para una red de 1.500 IPs máximas.
c. Módulo de investigación completa de amenazas: Licencia Cyber AI Analyst de Darktrace o equivalente para una red de 1.500 IPs aprox.

c) Implementación de una aplicación móvil para los administradores de la red con envío de las alertas de seguridad detectadas en tiempo real, facilitando la detección de problemas al personal técnico de la APB. Posibilidad de funcionamiento de la aplicación simultáneamente en los terminales a definir por la APB,

d) Puesta en marcha de la solución, incluyendo la implementación y su configuración

e) Servicio de soporte y apoyo continúo estándar:

El adjudicatario proveerá un servicio de asistencia y soporte durante toda la vigencia del contrato. Dicho servicio se basará como mínimo en la implementación de:

a. Soporte telefónico (hotline support): para soporte y asistencia a la APB vía teléfono, realizado por personal técnico de soporte del fabricante de la solución, disponible en horario 24/7.

b. Portal Web de cliente: para soporte y asistencia a la APB vía portal web, mediante apertura de tickets, realizado por personal técnico del fabricante de la solución, disponible en horario 24/7.

f) Servicio de soporte por expertos 24/7:

Servicio disponible desde el Portal Web de cliente, por el cual se ofrezca soporte por grupo de expertos a la APB en el proceso de análisis de investigación de amenazas, con el objetivo de entender correctamente las amenazas, flujos de datos, patrones existentes, acciones realizadas por módulo de respuesta autónoma, etc. Así como cualquier cuestión relacionada con la solución que la APB requiera.

Será un servicio con respuesta inmediata 24/7 los 365 días del año, por parte del grupo de expertos.

Este servicio será contratado obligatoriamente por la APB los 12 primeros meses meses del contrato, y **opcionalmente** podrá ser prorrogado los meses que requiera la APB según sus necesidades. Por tanto la APB, no estará obligada a una continuidad de la contratación de este servicio más de los 12 primeros meses.

g) Servicio 24/7 de monitorización y notificación proactiva de amenazas:

Mediante un SOC (*Security Operations Center*), el fabricante de la solución ofrecerá un servicio 24/7 de monitorización proactiva de amenazas significativas o de alto-medio impacto con aviso inmediato a personal de la División de Sistemas de APB. La notificaciones podrán serán vía SMS, llamada o emails, según lo acordado con la APB.

Las amenazas a notificar deberán ser verificadas previamente y confirmadas por los expertos del SOC de este servicio, de modo que se minimicen las falsas alarmas notificadas.

Una vez notificadas las amenazas, el servicio proveerá soporte completo y toda la información necesaria para que la APB lleve a cabo las acciones necesarias.

h) Servicio de mantenimiento completo de todo el hardware instalado durante toda la vigencia del contrato:

El adjudicatario supervisará continuamente el funcionamiento y rendimiento de los elementos hardware implementados, de modo que se garantice su correcto estado y funcionamiento durante toda la vigencia del contrato.

En caso de avería hardware, el adjudicatario se comprometerá al envío inmediato de equipo/s de sustitución hasta la reparación del hardware averiado, de modo que se minimice al máximo el tiempo de indisponibilidad del servicio. Todos los costes asociados a este mantenimiento (incluidos los de envío) serán a cargo del adjudicatario

Asimismo, el adjudicatario se comprometerá a la sustitución del hardware por otro con prestaciones superiores en el caso que las actualizaciones software lo requieran.

i) Actualizaciones continuas del software durante toda la vigencia del contrato:

Se ofrecerán e implementarán todas las actualizaciones y correcciones de errores disponibles de los módulos software implementados, de modo que la APB disponga siempre de las mejores prestaciones de la solución

j) Realización de curso de entrenamiento para los técnicos de la División de Sistemas de Información e Infraestructuras TIC:

Al inicio del contrato, el adjudicatario realizará un curso de entrenamiento completo de la solución a los técnicos designados por la APB sobre las características de la solución, configuración, funcionamiento de los distintos módulos e interpretación de los resultados. Además, se explicará el funcionamiento y mecanismos de notificación con los diferentes servicios contratados.

Las fechas, duración y contenido exacto del curso será acordado con los técnicos de la APB, previa propuesta del adjudicatario.

Este cursó se realizará únicamente una vez, en el primer año, al inicio del contrato

3.3. DESCRIPCIÓN DE LAS CARACTERÍSTICAS DE LOS MÓDULOS DE LA HERRAMIENTA

La solución a implementar se basará en una herramienta que dispondrá al menos de los siguientes módulos:

- Módulo de detección de red
- Módulo de respuesta autónoma
- Módulo de investigación completa de incidentes

A continuación se indica por separado las características de cada uno de los anteriores módulos:

MÓDULO DE DETECCIÓN DE RED

Este módulo será capaz de detectar las señales sutiles de una amenaza sin depender de reglas, firmas o suposiciones previas. Es decir, la detección no se debe basar en la definición previa de “comportamiento maliciosos” con reglas o firmas como medio para identificar las amenazas cibernéticas (no es un enfoque heredado), dado que las ciberamenazas avanzadas (en constante evolución) no se pueden anticipar por adelantado. Así, las características más relevantes que deberá disponer este módulo son:

- Auto - aprende ‘de forma continua’: adaptándose constantemente, analizando los ‘patrones de vida’ en profundidad.
- Unificada y ampliable: unifica distintas fuentes de datos en todo el negocio.

- Comprende a las personas: no solo a la tecnología, sino también el comportamiento de las personas.

De esta manera, este módulo debe realizar una compresión personalizada de los procesos y características de funcionamiento de la APB, para permitir la detección temprana de amenazas. Así se podrá proteger la red de amenazas novedosas, como personas internas malintencionadas y terceros, ataques de día cero y otros tipos de incidentes que evaden las reglas y los métodos de protección basados en firmas.

MÓDULO DE RESPUESTA AUTÓNOMA

Este módulo estará basado en una tecnología de respuesta autónoma. De este modo, el sistema no sólo detectará señales de amenazas, sino también proveerá una solución para luchar de manera inteligente contra los ataques en curso antes de que puedan tener cualquier impacto. Así, tomará medidas rápidas y específicas para interrumpir los ataques con precisión, incluso si la amenaza es dirigida o completamente desconocida.

Este módulo no generará cuarentenas generales que puedan causar más interrupciones, sino que funcionará aplicando quirúrgicamente el "patrón de vida" normal de un dispositivo infectado o usuario comprometido, neutralizando la amenaza en segundos y manteniendo las operaciones normales de negocio. Estas acciones autodirigidas no solo serán granulares, sino que también se adaptarán dinámicamente a la forma y gravedad de la amenaza a medida que se desarrolla.

Más allá de esta protección táctica, este módulo también podrá ofrecer una respuesta estratégica al actuar como el "cerebro de IA" de todo el equipo de seguridad, aprovechando las detecciones de alta confianza para transferir e integrar con las defensas en línea como mecanismo de respuesta. A través de integraciones activas, este módulo podrá conectarse sin problemas y mejorar el ecosistema existente, informando a los firewalls y dispositivos de red sobre los ataques que se han producido.

MÓDULO DE INVESTIGACIÓN COMPLETA DE AMENAZAS

Este módulo utilizará tecnología IA para proporcionar una investigación completa de los incidentes. Partiendo de un gran conjunto datos previos (obtenidos a través de otras implementaciones del sistema), este módulo tecnológico, ejecutará investigaciones de expertos a velocidad de máquina, correlacionando eventos a lo largo de toda la infraestructura y obteniendo conclusiones. Así se podrán lograr ahorros de tiempo significativos para los analistas de seguridad de la APB.

Este módulo podrá correlacionar de forma inteligente puntos de datos dispares en el negocio digital, lo que ayudará al equipo de seguridad de la APB a investigar las amenazas de manera más rápida y eficiente.

Mediante el uso de varias formas de aprendizaje automático, incluido el aprendizaje profundo, supervisado y sin supervisión, la tecnología ha aprendido la intuición humana y el oficio de cientos de analistas de clase mundial, pero potenciado por una IA y un aprendizaje automático mediante machine learning.

3.4. ACEPTACIÓN Y PRUEBAS

El adjudicatario deberá comunicar el momento de la puesta en marcha y disponibilidad de los sistemas y servicios a la APB para que sus técnicos den su aprobación, tras haber verificado la corrección de los mismos.

El objetivo de las pruebas es !a verificación de la disponibilidad de los servicios contratados y su calidad.

4. PLAZO PARA LA EJECUCIÓN DEL CONTRATO

El plazo para la ejecución del contrato será de **DOS (2) AÑOS**, a partir del Acta de Inicio del Servicio. Además, se establece dos posibles prórrogas de **UN (1) AÑO** cada una.

5. PRESUPUESTO

El **Presupuesto Base de Licitación** es **de CIENTO NOVENTA Y OCHO MIL QUINIENTOS NOVENTA Y DOS euros con CUARENTA Y SÉIS céntimos (198.592,46 €),** de los que **TREINTA Y CUATRO MIL CUATROCIENTOS SESENTA Y SEIS euros con CUARENTA Y SEIS (34.466,46 €)** corresponden al **21% de IVA**.

Siendo el **Valor Estimado del Contrato CUATROCIENTOS TREINTA Y SEIS MIL CUATROCIENTOS SETENTA Y NUEVE EUROS con NOVENTA Y UN céntimos (436.479,91 €),** de los que **SETENTA Y CINCO MIL SETECIENTOS CINCUENTA Y DOS euros con SETENTA Y UN céntimos (75.752,71 €)** corresponden al **21% de IVA**, **TREINTA Y DOS MIL OCHOCIENTOS VEINTICINTO euros con VÉINTE céntimos (32.825,20 €) al 20% de POSIBLE MODIFICACIÓN DEL CONTRATO**, **CIENTO SESENTA Y TRES MIL SETECIENTOS SETENTA Y SEIS euros (163.776,00 €)** a las **DOS posibles PRÓRROGAS DE UN AÑO CADA UNA**, habiéndose obtenido de acuerdo con el desglose que se presenta resumido en el cuadro adjunto:

Descripción producto	Unidad	Precio (€)	Importe Total (€)
Módulo de detección de red, Ref. Enterprise Immune System de Darktrace o equivalente. Módulo de investigación completa de amenazas, Ref. Cyber AI Analyst o equivalente incluidas actualizaciones y mejoras. Incluye: para 1.500 IPs máx., Incluye: - Puesta en marcha y configuración - Actualizaciones y mejoras - Servicio de soporte y apoyo continúo estándar Todo según los requisitos indicados en Pliego	24	3.742,00	89.808,00
Módulo de respuesta autónoma, Ref. Antigena Network de Darktrace o equivalente, para 1.500 IPs máx. Incluye: - Puesta en marcha y configuración - Actualizaciones y mejoras - Servicio de soporte y apoyo continúo estándar Todo según los requisitos indicaods en Pliego	24	1.142,00	27.408,00
Sistema Hardware, compuesto por: - Medium appliance para Palma - Small appliance para Maó - Small appliance para Eivissa Incluye: - Puesta en marcha y configuración - Actualizaciones y mejoras - Aplicación móvil para administadores de la red - Servicio de soporte y apoyo continúo estándar - Mantenimiento completo de todos los equipos Todo según los requisitos indicados en Pliego	24	320,00	7.680,00
20 Ud Client Sensors (agentes software) para los usuarios de las sedes de Alcudia y La Savina	24	20,00	480,00
Servicio 24/7 de monitorización y notificación proactiva de amenazas, según requisitos indicados en Pliego	24	800,00	19.200,00
Servicio de soporte por expertos 24/7, según requisitos indicados en Pliego	24	800,00	19.200,00
Curso de entrenamiento para técnicos de la APB, según requisitos indicados en Pliego (sólo primer año)	1	350,00	350,00

PRESUPUESTO BASE DE LICITACIÓN (2 AÑOS)	**164.126,00**
IVA (21%)	34.466,46 €
PRESUPUESTO BASE DE LICITACIÓN CON IVA (2 AÑOS)	**198.592,46**
Previsión Modificación Contrato hasta un máximoa del 20% (art. 204 LCSP)	**32.825,20**
TOTAL PRIMERA PRÓRROGA (1 AÑO) SIN IVA	81.888,00
TOTAL SEGUNDA PRÓRROGA (1 AÑO) SIN IVA	81.888,00
PRÓRROGAS (1 AÑO + 1 AÑO) SIN IVA	**163.776,00 €**
VALOR ESTIMADO CONTRATO (2 años + 1 AÑO + 1 AÑO+ 20% art. 204 LCSP)	**360.727,20 €**
IVA (21%)	75.752,71 €
VALOR ESTIMADO DEL CONTRATO IVA INCL:	**436.479,91 €**

Tal como se ha indicado, se prevé una modificación de contrato hasta un máximo del veinte por ciento (20%) del Presupuesto de Licitación (sin IVA), de acuerdo con lo señalado en el artículo 204 de la LCSP.

A continuación, se formula de forma clara, precisa e inequívoca la cláusula de modificación del contrato. La naturaleza de dichas modificaciones vendrá determinada por un posible aumento de número de direcciones IP de red o/o clientes sensores a monitorizar a medida que se incorporen a la red de la APB nuevos dispositivos.

Así, las condiciones en las que se verificará de forma objetiva la modificación del contrato serán las siguientes:

- Aumento del número de direcciones IP a analizar en el módulo de detección de red, y el módulo de respuesta autónoma.
- Aumento del número de clientes sensores (agentes software) para monitorizar la red

La modificación no podrá suponer el establecimiento de nuevos precios unitarios no previstos en el contrato.

La empresa adjudicataria percibirá de la APB el importe por ella ofrecido en su proposición económica. Se efectuarán pagos mensuales, debidamente justificados y documentados, según los servicios realmente prestados.

En el precio del Contrato estarán incluidos todos los gastos de desplazamientos y dietas (si procediera) y otros costes complementarios (ej. Envío del hardware), necesarios para la ejecución del contrato.

6. PLAZO DE GARANTÍA

Dada la naturaleza de este contrato (servicio), no se establece plazo de garantía.

7. PRESCRIPCIONES TÉCNICAS GENERALES

Por su carácter general se considerarán vigentes y de aplicación las siguientes disposiciones, normas e instrucciones, que complementan el presente Documento en lo referente a aquellos aspectos no mencionados expresamente en él, quedando a juicio del Director dirimir las posibles contradicciones habidas entre ellas.

- 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 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante
- 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 UNE aplicables a equipos y materiales.

- Normas N.T.E., normas UNE, normas DIN e ISO.

Así como la Legislación que sustituya, modifique o complete las disposiciones citadas y la nueva Legislación aplicable que se promulgue, siempre que esté vigente con anterioridad a la fecha del Contrato

8. CONDICIONES GENERALES

8.1. MEDIDAS DE SEGURIDAD

El Adjudicatario será responsable de las condiciones de seguridad en los trabajos, estando obligado a adoptar y hacer aplicar, a su costa, las disposiciones vigentes sobre esta materia, las medidas que puedan dictar el Ministerio de Trabajo y Economía Social y demás Organismos competentes en materias de Seguridad e Higiene en el Trabajo y las normas de seguridad que correspondan a las características de los mismos.

8.2. GASTOS DE CARÁCTER GENERAL A CARGO DEL CONTRATISTA

Cualquier tipo de gasto no especificado será por cuenta del adjudicatario, de acuerdo con la legislación vigente.

En los casos de resolución del contrato, cualquiera que sea la causa que la motive, serán de cuenta del adjudicatario los gastos originados por la liquidación de los mismos.

Dado que no es necesario efectuar modificaciones en la infraestructura de las instalaciones técnicas de la APB se exime de la obligatoriedad de constituir fianza.

8.3. MEDICIÓN Y ABONO DE LOS TRABAJOS

Los trabajos se abonarán por unidad realmente ejecutada. Las unidades se medirán en función de la descripción que figura en el presente documento, una vez comprobada su idoneidad, formándose la correspondiente “Relación Valorada”, aplicándose al efecto los precios unitarios contractuales afectados por la baja de adjudicación. La relación valorada para la certificación de los trabajos será mensual.

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

Las facturas se abonarán previa presentación en FACe, previa certificación correspondiente conforme a las instrucciones de la APB al respecto.

No procederá, durante todo el plazo contractual la revisión de precios al contratista adjudicatario.

8.4. CONTRADICCIONES Y OMISIONES DEL PRESENTE DOCUMENTO

Las omisiones erróneas de los detalles que sean indispensables para llevar a cabo el espíritu e intención expuestos en estas especificaciones, o que, por uso y costumbre deban ser realizados, no sólo no exime al Contratista de la obligación de ejecutar estos detalles de omitidos o erróneamente descritos, sino que por el contrario, deberán ser ejecutados como si hubieran sido completos y correctamente especificados en este documento.

8.5. 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 establecidas el Contratista para la prestación de servicios a personas físicas o jurídicas privadas siendo en todo caso de aplicación al contrato cuanto previene la normativa vigente.

Palma, a fecha de firma del documento

El autor del documento,
EL RESPONSABLE DE DIVISIÓN DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURAS TIC

José Miguel Esteve Lledó
Ingeniero de Telecomunicación

Revisado,
EL JEFE DE DIVISIÓN DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURAS TIC

Javier Segovia Mascaró
Ingeniero Informático

VºBº,
EL JEFE DE ÁREA DE PLANIFICACIÓN E INFRAESTRUCTURAS

Antonio Ginard López
Ing. de Caminos, Canales y Puertos

VºBº,
EL DIRECTOR DE LA APB

Jorge Nasarre López
Ing. de Caminos, Canales y Puertos