Expediente P.O.54.22

Pliego de Prescripciones Técnicas para la adquisición, instalación y configuración y puesta en marcha de una plataforma de seguridad en el puesto de trabajo y en los servidores de la red corporativa de la Autoridad Portuaria de Baleares

Índice

1 Antecedentes y justificación

La Autoridad Portuaria de Baleares (en adelante APB) precisa tener disponible 24x7 una herramienta que garantice protección centralizada para los puestos de trabajo y servidores de su red corporativa conectados contra todo tipo de amenazas en Internet, incluyendo virus, programas espía, ataques piratas y correo electrónico.

En la actualidad la APB dispone de licencias del antivirus Kaspersky, que finalizan el próximo 17 de octubre de 2022.

Es por ello, que la APB necesita un sistema avanzado de detección y respuesta de amenazas de tipo XDR (Cross Detection and Response), que integre inteligencia tanto de red como del puesto de trabajo. Esta solución será capaz de almacenar y correlar los logs de ambos entornos y, de manera automatizada, generar inteligencia desde los mismos para identificar las amenazas más relevantes, simplificando su gestión y disminuyendo el tiempo de respuesta a los incidentes, incluso de forma automática tomando medidas reactivas.

2 Objeto del contrato

El objeto del contrato es la adquisición, instalación y configuración y puesta en marcha de una plataforma de seguridad en el puesto de trabajo y en los servidores de la red corporativa de la APB, así como el soporte y mantenimiento de la nueva plataforma durante todo el período de vigencia del contrato.

El objetivo es incorporar funcionalidades de nueva generación dotando a la red corporativa de la APB, que cuenta con distintas sedes (Palma, Maó, Eivissa, Alcúdia y La Savina), con medidas de protección y seguridad más avanzadas que hagan frente a los crecientes riesgos de seguridad, con capacidades de Inteligencia Artificial y automatización de las medidas de protección.

A continuación, se resumen las características principales que se pretenden obtener con el despliegue de dicha solución en la APB:

- Detección automatizada de amenazas enmascaradas.
- Reducción del tiempo medio de identificación de amenazas (MTTI – Mean Time To Identify).
- Disminución del tiempo medio para la respuesta (MTTR – Mean Time To Response).
- Visión completa de la amenaza, incluyendo la cadena de causalidad, es decir determinar su procedencia y mecanismo de generación e infección.
- Optimización del volumen de alertas de seguridad y su gestión, gracias al análisis automatizado de las causas principales.
- Recopilación de información para un posible análisis forense.
- Pivotaje entre evidencias obtenidas a través de datos de múltiples fuentes y datos obtenidos de los endpoints indistintamente.

3 Descripción de los servicios. Requerimientos y especificaciones de los servicios

Las prescripciones técnicas que se marcan a continuación, son requisitos mínimos, de tal modo que su incumplimiento determinará la desestimación de la oferta presentada.

Con el objetivo de clarificar la solución a suministrar y dado que no siempre es posible realizar una descripción lo bastante precisa e inteligible que contemple todas las características técnicas y exigencias funcionales requeridas, se agrega al final de la descripción técnica de cada elemento la referencia de un producto concreto comercial. No obstante, las referencias a marcas y modelos que aparecen en estas características técnicas y en las mediciones **no son en ningún caso excluyentes**, sino que pretenden establecer los criterios de diseño, los niveles de calidad y las prestaciones mínimas que se exigirán a la plataforma de seguridad, por lo que las empresas licitadoras podrán presentar ofertas con productos equivalentes, siempre y cuando acrediten perfectamente que las características ofertadas son equivalentes técnicamente con las especificadas en el Pliego. Todas ellas serán tomadas en consideración, siempre que:

- No se aparten sustancialmente de las funcionalidades especificadas y operación del sistema, según se describen en este Pliego.
- Sean equivalentes o superiores en prestaciones y calidad a los referenciados en el Pliego, o aporten alguna ventaja funcional importante.
- Queden suficientemente justificadas desde el punto de vista técnico.

No se considerará equivalente y no se admitirá el producto ofertado si todas o alguna de las especificaciones son de menor calidad que el presentado en el presente Pliego.

3.1 Suministros

El objetivo del suministro es una plataforma de seguridad que dé respuesta a la problemática de los actuales sistemas EDR (Extended Detection and Response), que trabajan aislados de los sistemas de detección en red, mediante el suministro, instalación avanzada, configuración y explotación para la APB de un sistema avanzado de detección y respuesta de amenazas de tipo XDR (Cross Detection and Response), que integre inteligencia tanto de red como de puesto de trabajo/endpoint.

Los elementos principales que deben componer la solución son los siguientes:

- **Agente del endopint XDR:** Este agente alimentará el servicio con la información pertinente del puesto de trabajo, la solución debe tener capacidades de prevención y respuesta integradas.
- **Sensores de tráfico red XDR:** Se deberá integrar con los principales fabricantes de firewalls de nueva generación.

  Además de actuar como sensores y recopilar la información de la red, estos sistemas deben ofrecer la capacidad de responder a los incidentes conforme a la decisión tomada por los administradores de la solución. Para cumplir este punto, es

imprescindible que la solución sea abierta y permita integrar logs/alertas de soluciones de distintos fabricantes.

- **Base de datos de logs integral:** Se precisa una base de datos integral basada en la nube para los registros enriquecidos con información contextual que generan los firewalls de nueva generación, los agentes del endpoint y cualquier log de terceros tanto on premise como en la nube.

  Por lo menos, la base de datos de logs integral debe almacenar los datos de toda la telemetría durante 30 días en caliente.

- **Aplicación XDR:** Se precisa de un único interfaz web en la nube para gestionar el servicio que permita aunar los logs y telemetría de los distintos sensores y agentes y que, utilizando algoritmos basados en inteligencia artificial detecte automáticamente las amenazas, clasificándolas y agrupándolas por incidentes, permitiendo realizar la gestión y respuesta.

Esta solución será capaz de almacenar y correlar (comparar) los logs (registros) de ambos entornos y, de manera automatizada, generar inteligencia desde los mismos para identificar las amenazas más relevantes, simplificando su gestión y disminuyendo el tiempo de respuesta a los incidentes, incluso de forma automática tomando medidas reactivas.

Asimismo, la plataforma de seguridad propuesta deberá acompañarse de un servicio de instalación avanzada con el objetivo de que la APB adquiera capacidades de detección proactiva y respuesta de las amenazas. La empresa licitadora deberá explotar la solución y prestar servicios de tipo detección proactiva, así como proporcionar un servicio integrado de auditoría continua y soporte.

Finalmente, la plataforma de seguridad deberá ir acompañada de todos los servicios de gestión y explotación de la información y la inteligencia generada.

Por lo tanto, se requiere el suministro, instalación, configuración y puesta en marcha de una plataforma de seguridad con las características siguientes:

- 500 licencias de la solución XDR, que incluiría las funcionalidades de capacidades de prevención antimalware y antiexploit, sandboxing y motor local (Machine Learning), cifrado de equipos, host firewall, control de dispositivos externos, período de retención de 30 días y identity analytics.

  Adicionalmente, se podrán contratar hasta un máximo de 100 licencias en caso de necesidad.

- 500 licencias de Host Insights, que incluiría las funcionalidades de inventariado de activos, análisis de vulnerabilidades y la capacidad de Search & Destroy.

  Adicionalmente, se podrán contratar hasta un máximo de 100 licencias en caso de necesidad.

- 5TB para la ingesta y análisis de logs de diferentes fuentes (red, nube, identidad y otras fuentes) o equivalente, proporcionando contexto adicional sobre las alertas existentes de los endpoint.

- Servicio de soporte Premium, con soporte telefónico 24x7 y gestión de tickets ilimitada, acceso al portal de atención al cliente, a la base de conocimientos y a la documentación en línea.
- Servicio de Mananged Threat Hunting, realizado por analistas del fabricante, mediante el cual se realizan búsquedas proactivas y de manera continuada para buscar amenazas dentro de la red corporativa.

Los requisitos de la solución XDR, el paquete Host Insights, el servicio de soporte Premium y el servicio de Managed Threat Hunting que se deberán cumplir se detallan en el ANEXO I. Requisitos de la solución XDR.

3.2 Soporte y mantenimiento

La empresa adjudicataria deberá proporcionar, instalar y configurar las actualizaciones de software a la última versión liberada y estable del fabricante en el momento de la adjudicación del contrato, de todos los productos objeto de esta contratación, garantizando la compatibilidad con el resto de los componentes, y dada la criticidad de este sistema, mantenerlo siempre en la última versión proporcionada por el fabricante.

La empresa adjudicataria deberá prestar un **servicio de Threat Hunting** sobre el XDR desplegado en el que al menos se definan casos de uso, indicadores de compromiso y enriquecimiento de datos. El servicio de Threat Hunting es el proceso mediante el cual se realizan búsquedas proactivas y de manera continuada para buscar amenazas dentro de la red corporativa. Esta aproximación está basada en hipótesis y no centradas en las alertas que ya se están gestionando a través de los logs y alertas generados por los sistemas de monitorización disponibles en una organización.

La adquisición de capacidades de detección proactiva deberá permitir a la APB con capacidades para:

- Aplicar medidas correctivas.
- Aplicar seguridad en la red y en los dispositivos.
- Evaluación de efectividad de los productos desplegados en la APB.
- Enriquecimiento en las áreas que necesitan un mayor foco relacionado con ciberseguridad.

Asimismo, la empresa adjudicataria deberá prestar un **servicio de soporte al seguimiento y gestión del ciclo de vida de las vulnerabilidades** y propuesta de corrección y planes de actuación a partir de los resultados, de forma que el conocimiento y los resultados del XDR sea utilizado para una gestión con visión única de la seguridad en la red y los dispositivos de la APB.

La empresa adjudicataria está comprometida a garantizar la calidad del servicio, a cumplir los Acuerdos de Nivel de Servicio (ANS) y a documentar e informar de su cumplimiento o incumplimiento a la APB. El incumplimiento de los ANS originará las penalizaciones adecuadas, es decir, en caso de no dar un servicio de calidad se realizará un descuento en la facturación.

Cuando ocurra cualquier tipo de incidencia relacionada con el objeto del contrato, la empresa adjudicataria deberá de resolver dicha incidencia en como máximo los sucesivos tiempos de respuesta y resolución reflejados en la siguiente tabla dependiendo de su nivel de gravedad.

Se considera tiempo de respuesta al tiempo que transcurre desde la comunicación de la incidencia (por la vía acordada con la empresa adjudicataria) hasta el inicio por parte del servicio de soporte de la empresa adjudicataria, de la actividad necesaria para la resolución de la incidencia, dando lugar a la conexión remota con el sistema afectado, o a la visita de un técnico experto, si esto fuera necesario.

Se considera tiempo de resolución al período de tiempo transcurrido desde que se detecta una incidencia de forma proactiva por parte de la empresa adjudicataria o la APB comunica a la empresa adjudicataria la incidencia, hasta el momento en que queda solucionada.

Para el entorno de producción se establecen los siguientes niveles de servicio. En caso de no cumplir con los tiempos de resolución establecidos se podrán derivar las siguientes penalizaciones. La penalización se refiere a cada incidencia cuyos tiempos de resolución no se cumplan.

Nivel de gravedad	Tiempo de respuesta	Tiempo de resolución	Penalización en tiempo de resolución
Crítica	Antes de 1 hora	Antes de 6 horas	50€/hora retraso
Grave	Antes de 3 horas	Antes de 24 horas	25€/hora retraso
Normal	Antes de 6 horas	Antes de 72 horas	10€/hora retraso

Se considera la posibilidad de las incidencias siguientes, que se clasifican según el nivel de gravedad:

i. **Incidencia crítica:** el servicio o la aplicación no funciona. Implica una parada o una distorsión grave en la operativa normal de funcionamiento del sistema.

ii. **Incidencia grave:** el servicio o la aplicación o una de sus funcionalidades tiene una anomalía importante, pero no impide la operativa normal del resto de funcionalidades.

iii. **Incidencia normal:** el servicio o la aplicación o una de sus funcionalidades tiene una incidencia, pero se puede usar con normalidad.

Las incidencias se comunicarán por parte de la APB al Jefe/a de proyecto de la empresa adjudicataria al correo electrónico que se indique a tal efecto. En caso de incidencias críticas también se intentará contactar por teléfono, por lo que el Jefe/a de proyecto deberá indicar un número de teléfono en el que esté disponible en horario laboral (se establece el horario laboral en los días laborables en Palma en horario de 8:00 a 18:00).

La empresa adjudicataria propondrá el sistema y procedimientos de gestión de las incidencias en el marco de la presente asistencia técnica.

Las **tareas de soporte** se realizarán mediante los siguientes mecanismos:

- **Soporte por correo electrónico.** La empresa adjudicataria deberá proveer un correo electrónico de soporte, al cual responder y resolver las incidencias y dudas que se envíen por parte del personal de Sistemas de Información e Infraestructuras TIC.
- **Soporte telefónico.** 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 24x7** para dar soporte al personal de Sistemas de Información e Infraestructuras TIC.
- **Soporte presencial.** La empresa adjudicataria realizará el soporte presencial y asistencia técnica in situ en las instalaciones de la APB, en caso necesario y siempre que la situación lo permita, para conseguir una atención inmediata y personalizada. Este soporte presencial consistirá como mínimo en la presencia de cinco (5) días hábiles anuales en jornada completa, que se distribuirán de forma conjunta o separada, en función de las necesidades del servicio, a juicio del Responsable del Contrato.

  La planificación y coordinación de estas jornadas in situ serán aprobadas por el Responsable del Contrato.

Todos los tiempos de respuesta y resolución serán computados a través de una aplicación de gestión de incidencias (JIRA o equivalente), que proporcionará la empresa adjudicataria a la APB, sin coste adicional para la APB, en ningún caso.

3.3 Gestión del cambio y formación

La empresa adjudicataria deberá realizar la gestión del cambio y la formación necesaria para posibilitar la gestión de la plataforma de seguridad en la APB.

Para ello deberá elaborar un plan de formación que incluya al menos formación básica y avanzada en la plataforma de seguridad. Esta formación irá dirigida al personal de Sistemas de Información e Infraestructuras TIC.

La estimación definitiva del número de sesiones formativas, su duración, contenidos, número y perfil de los asistentes, así como aquellos aspectos no especificados, se determinará en base a las necesidades detectadas por la APB para la correcta gestión de la plataforma de seguridad. Dichas sesiones dirigidas al personal de Sistemas de Información e Infraestructuras TIC, supondrán un mínimo de diez (10) horas de formación.

Como norma general, todas las sesiones de formación incluirán la entrega de documentación al inicio de las mismas para todos los participantes. La APB podrá grabar dichas sesiones para ponerlas a disposición de su personal.

4 Entregables

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

La documentación generada durante la ejecución del contrato será de propiedad exclusiva de la APB sin que los adjudicatarios puedan 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 los adjudicatarios con expresión del fin.

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

Soporte y mantenimiento

i. Manuales de instalación y configuración.

ii. Servicio de Threat Hunting (notificación de vulnerabilidades, información de campañas/actividades maliciosas, incluyendo información sobre nuevas amenazas, normativas e incidentes destacados).

iii. Servicio de soporte al seguimiento y gestión del ciclo de vida de las vulnerabilidades (informes de amenazas, informes de consultas e informes de impacto).

iv. Informes de servicio (volúmenes de llamadas, consultas, incidencias y peticiones de cambios, ANS).

Gestión del cambio y formación

v. Identificación de necesidades.

vi. Plan de formación detallado, que se deberá consensuar y aprobar por parte de la APB.

vii. Informes de las acciones de formación realizadas (sesiones, asistentes, contenido, incidencias, encuesta de satisfacción...).

viii. Documentación utilizada para realizar las acciones de formación.

5 Plazo para la ejecución del contrato

El plazo de ejecución del contrato se establece en un plazo máximo de TREINTA Y OCHO (38) MESES desde el acta de inicio de los trabajos (reunión de kick-off).

La implantación, configuración y puesta en marcha de la plataforma de seguridad se realizará en un plazo máximo de DOS (2) MESES, correspondiendo el resto del plazo de TREINTA Y SEIS (36) MESES a la operación, soporte y mantenimiento de la plataforma de seguridad.

El desarrollo de los trabajos se realizará en los locales de la empresa adjudicataria con sus propios recursos físicos y lógicos. 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. Cabe tener en cuenta que la APB cuenta con distintas sedes (Palma, Maó, Eivissa, Alcúdia y La Savina).

6 Presupuesto, recepción de los trabajos y forma de pago

6.1 Presupuesto máximo de licitación

El presupuesto de licitación excluido IVA es de DOSCIENTOS SESENTA Y DOS MIL OCHOCIENTOS EUROS (262.800,00 €), resultando el IVA (21%) CINCUENTA Y CINCO MIL CIENTO OCHENTA Y OCHO EUROS (55.188,00 €) y el Presupuesto de Ejecución por Contrata de TRESCIENTOS DIECISIETE MIL NOVECIENTOS OCHENTA Y OCHO EUROS (317.988,00 €).

El presupuesto de licitación se desglosa en el siguiente cuadro:

Ud.	Concepto	Nº Ud.	€/Ud.	Total	%
Año	**Suministros**		**57.600,00 €**	**172.800,00 €**	**67,75%**
Año	Solución XDR (500 licencias)	3	20.000,00 €	60.000,00 €	22,83%
Año	Host Insights add-on Solución XDR (500 licencias)	3	3.000,00 €	9.000,00€	3,42%
Año	Solución XDR (100 licencias adicionales - partida opcional)	3	4.000,00 €	12.000,00 €	4,57%
Año	Host Insights add-on Solución XDR (100 licencias adicionales - partida opcional)	3	600,00 €	1.800,00€	0,68%
Año	Solución XDR, 5TB de base de datos de *logs* integral	3	30.000,00 €	90.000,00 €	34,25%
Año	**Soporte y mantenimiento**		**29.000,00 €**	**87.000,00 €**	**33,11%**
Año	Servicio de soporte Premium	3	15.000,00 €	45.000,00 €	17,13%
Año	Servicio de Threat Hunting	3	14.000,00 €	42.000,00 €	15,98%
Año	**Gestión del cambio y formación**	**3**	**1.000,00 €**	**3.000,00 €**	**1,14%**
	TOTAL PRESUPUESTO CONTRATO (sin IVA)			**262.800,00 €**	**100,00%**
	IVA	**21%**		**55.188,00 €**	
	PRESUPUESTO EJECUCIÓN CONTRATO (con IVA)			**317.988,00 €**	

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.

6.2 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**.

6.3 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".

7 Garantía

Se fija un periodo de garantía de VEINTICUATRO (24) MESES sobre los trabajos realizados en el ámbito de este contrato, contados desde la fecha de firma del acta de finalización del contrato, y durante los cuales la empresa adjudicataria se hace responsable de la resolución de las incidencias que éstos puedan generar y de la corrección de cualquier problema de funcionamiento que pudiera detectarse.

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

8 Normativa de aplicación

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

Así como cuanta normativa desarrolle, amplíe o sustituya a la antes citada. No obstante, deberá consultarse, las posibles actualizaciones de la mencionada normativa.

9 Seguridad

9.1 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, el adjudicatario 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 Desarrollo software

Para el desarrollo de software objeto del contrato, la empresa adjudicataria deberá utilizar una metodología de desarrollo software y unas reglas de codificación segura para garantizar que el software desarrollado no contiene vulnerabilidades. Se deberá mencionar explícitamente:

- Cómo se tiene en cuenta la seguridad de la información durante todo el ciclo de vida del desarrollo.
- Cómo se utilizarán los datos de prueba en caso de ser datos reales.
- Si se utilizan lenguajes que permitan la inspección del código fuente en caso de ser necesario.

Previo a su entrega, el software desarrollado será objeto de pruebas funcionales y pruebas de seguridad por parte del adjudicatario, de forma que se verifique que los requisitos funcionales y de seguridad se cumplen satisfactoriamente. La empresa adjudicataria deberá realizar un

plan de pruebas formales, donde se describan los casos de prueba, las condiciones de la prueba, las entradas inyectadas, los resultados esperados y los resultados obtenidos. El plan de pruebas, junto con sus resultados, será entregado a la APB junto con las entregas de software a las que hace referencia.

9.8 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.

10 Contraindicaciones 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.

11 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 la empresa adjudicataria 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 a la empresa adjudicataria de la obligación de su cumplimiento.

Palma, a fecha de firma del documento

Autor del Documento

Francesc Piris Pons
Responsable Sistemas de Información e Infraestructuras TIC

Conforme,

Javier Segovia Mascaró
Jefe de División de Sistemas de Información e Infraestructuras TIC

VºBº,

Antonio Ginard López
Jefe de Área de Planificación e Infraestructuras

VºBº,

Jorge Nasarre López
Director

ANEXO I. Requisitos de la solución XDR

I.1. Agente del endpoint XDR

El agente del endpoint XDR deberá cumplir los siguientes requisitos:

Requisito	Descripción
REQ-01	Se requerirá la instalación de un único agente que permita realizar tanto las tareas de recopilación de información como las de respuesta. El agente debe incluir capacidades de prevención avanzada frente a malware/exploits desconocidos (zero day).
REQ-02	El servicio de detección y respuesta deberá recolectar información y datos de telemetría que lleguen a nivel de hilo (thread) de un proceso.
REQ-03	El agente deberá soportar la recolección continuada de los datos a nivel del sistema, aplicación y usuario siendo capaz de recolectar al menos los siguientes eventos: • Eventos de creación y terminación de procesos. • Modificaciones del registro. • Carga de imágenes. • Información de conexión/desconexión de sesiones. • Logon/Logoff. • Creación/modificación/lectura de ficheros. • Sesiones en red. • Arranque de un equipo. • Cambio de hora en el equipo.
REQ-04	El agente propuesto en los endpoints deberá poder extender las capacidades UEBA (User Entity Behavior Analytics) y NTA (Network Traffic Analysis)/NDR (Network Detect & Response), obtenidas desde el análisis de logs de red, aprovechando la recolección de los datos y proporcionando contexto adicional sobre las alertas existentes. No se requiere actualmente la integración del tráfico de red en la solución XDR, sino que debe estar disponible para incorporar a futuro.
REQ-05	En lo que a la respuesta se refiere, se deberá poder realizar al menos las siguientes acciones de respuesta: • Aislar un endpoint. • Escanear. • Poner en cuarentena ejecutables involucrados en un incidente. • Terminar procesos involucrados en un incidente.

	• Ejecutar un terminal remoto seguro desde la consola de administración que permita al menos gestionar los procesos en ejecución, sistema de ficheros y ejecutar comandos/scripts de forma remota tanto para Windows como Linux y Mac.
	• Generar listas dinámicas con IOCs que puedan ser consumidos por los cortafuegos de red u otros elementos de red para complementar su política de enforcement.
	• Remediar cambios de actividad maliciosa, enumerando qué archivos y claves de registro desencadenaron la cadena de causalidad, disponiendo de sugerencias de corrección de al menos:
	  ○ Terminar cadena de causalidad.
	  ○ Borrar archivo.
	  ○ Restaurar archivo.
	  ○ Renombrar archivo.
	  ○ Eliminar valor de registro.
	  ○ Restaurar valor de registro.
	• Ejecutar un script, tanto desde un repositorio de la herramienta, con scripts preestablecidos, como tener la posibilidad de añadir nuevos scripts en python. Debe permitir tratar de manera especial los scripts de alto riesgo para prevenir daños en el sistema.

REQ-06	La solución deberá poder desplegarse desde Directorios Activos, mediante un ejecutable ligero. Es necesario disponer del instalador en formato MSI para que pueda ser distribuido bien usando políticas GPO (Group Policy Objet) de Directorio Activo u otras herramientas de distribución similares. Así mismo, la herramienta deberá permitir actualizar manual y automáticamente los agentes ya desplegados.
Ref.	Cortex XDR PRO o equivalente (500 licencias + 100 licencias adicionales).

I.2. Sensores de tráfico red XDR

Los sensores de tráfico red XDR deberán cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-07	La solución deberá ser compatible con los firewalls de nueva generación de los principales fabricantes.
REQ-08	Las sondas deberán ser capaces de recopilar la información que requieran para su funcionamiento sin necesidad de descifrar el tráfico SSL.
REQ-09	Los sensores deberán ser capaces de actuar con los elementos de red para ejecutar las acciones de respuesta, tales como el bloqueo de IPs o redes que se

	consideren comprometidas.
Ref.	Cortex XDR PRO o equivalente (500 licencias + 100 licencias adicionales).

I.3. Base de datos de logs integral

La base de datos de logs integral deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-10	La solución deberá ser una plataforma abierta con capacidad de incorporar logs desde otros entornos/fabricantes, con el fin de extender su funcionalidad en el futuro.
REQ-11	El servicio de recolección de la información deberá ser capaz de recolectar datos a gran escala, estando preparado para su aplicación en el análisis matemático y el big data.
REQ-12	La solución de base de datos deberá desplegarse fuera de las instalaciones de la APB, de modo que no sea necesario instalar almacenamiento en local, pero debe accederse desde los dispositivos de seguridad desplegados actualmente en la red de la APB.
REQ-13	El proveedor del servicio deberá poseer la **certificación SOC 2 Tipo II** para garantizar la seguridad física sobre los sistemas que van a almacenar los datos. Además, se deberá garantizar la privacidad de estos de modo que no puedan compartirse con otras empresas u organismos, tanto dentro como fuera de la Unión Europea.
REQ-14	La telemetría de los endpoints deberá recogerse de manera continua, **reteniendo al menos 30 días en caliente**, sin filtrar eventos (todos los accesos a ficheros, procesos, registros, etc.), siendo esta enviada independientemente de la existencia de alertas asociadas.
REQ-15	Se requerirán al menos 500 dispositivos protegidos con la solución y 30 días de almacenamiento, junto **con 5 TB de logs** provenientes de los firewalls de nueva generación. Además, el servicio de Managed Threat Hunting del fabricante.
REQ-16	La solución deberá poder ampliarse fácilmente si los requisitos de almacenamiento aumentan. Se valorará positivamente que la ampliación de almacenamiento sea transparente para la APB y que no requiera parada de servicio.
REQ-17	La base de datos deberá soportar al menos el protocolo Syslog (CEF, LEEF, CISCO, CORELIGH o RAW - UDP, TCP o Secure TCP, permitiendo fijar versión mínima de TLS 1.2), CSV, Bases de datos (MySQL, PostgreSQL, MSSQL u Oracle), Nube (AWS, Azure, Google), Ficheros y Carpetas, FTP, NetFlow y Windows Events, Http Listener, FileBeats o XDR Collectors.

REQ-18	Se requiere que todas las comunicaciones sean cifradas entre los componentes que forman parte del servicio de base de datos (tanto los de ingesta de *logs* como los de reenvío, con Syslog sobre TLS). Es necesario que los datos en tránsito sean encriptados utilizando al menos el método de encriptación TLS 1.2.
REQ-19	La base de datos deberá poder registrar toda la información de los eventos recibidos, independiente de la fuente, creando los datasets correspondientes que podrán ser consultados en raw o parseados.
REQ-20	El servicio deberá proporcionar procedimientos para alertar y soportar acciones preventivas ante un potencial fallo en el envío de logs.
Ref.	Cortex XDR PRO, 5TB de base de datos de logs integral o equivalente.

I.4. Aplicación XDR

La aplicación XDR deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-21	El sistema deberá ser capaz de acelerar las investigaciones recolectando información desde múltiples orígenes (red y endpoint al menos), para revelar la causa raíz de las alertas. No se requiere actualmente la integración del tráfico de red en la solución XDR, sino que debe estar disponible para incorporar a futuro.
REQ-22	Los datos recopilados deberán poder utilizarse para la detección basándose en artefactos, threat intelligence o analítica (machine learning/comportamiento).
REQ-23	La solución deberá permitir la detección de IOCs estáticos y de comportamiento (basados en TTPs y analíticas). Debe ser posible asimismo realizar búsquedas manuales de IOCs en la base de datos de forma que permita comprobar de una manera sencilla y directa la afectación de la organización a IOCs obtenidos desde esta aplicación u otra externa (por ejemplo, recibidas a través de un CERT o MSSP).
REQ-24	La solución deberá tener integrada una herramienta de inteligencia de amenazas para la identificación y clasificación del malware. Para garantizar la seguridad de esta herramienta, deberá tener la certificación FedRAMP. La FedRAMP (Federal Risk and Authorization Management Program) es un programa global del gobierno de los Estados Unidos que proporciona un enfoque estandarizado para la evaluación de la seguridad, la autorización y la supervisión continua de los productos y servicios en la nube.
REQ-25	La aplicación deberá ser capaz de realizar el profiling de los equipos, IPs y usuarios y calcular el baseline sobre el que detectar anomalías, utilizando para ello algoritmos de machine learning, que estudien al menos:

	• Comportamiento actual (actividad actual del usuario y del dispositivo). • Perfil temporal (actividad pasada del usuario y dispositivo). • Perfil de relación con otros peers. • Perfil de la entidad (tipo de dispositivo, usuario, ...).
REQ-26	La gestión de la solución deberá realizarse de manera centralizada a través de una consola única que integre la solución de protección de endpoints, así como la parte de análisis XDR.
REQ-27	El sistema de detección y respuesta deberá generar información forense relacionada con cada equipo de forma que pueda ser consultado posteriormente.
REQ-8	La solución deberá ser capaz de adaptar las defensas aplicando el conocimiento obtenido de investigaciones anteriores para la detección de futuras vulnerabilidades.
REQ-29	La solución deberá soportar RBAC (Role Based Access Control), para la identificación del nivel de acceso que un usuario puede tener sobre la aplicación. Estos roles podrán definirse de forma predefinida o personalizados y podrán aplicarse a un conjunto concreto de endpoints al menos para la administración, cuadros de mandos e informes.
REQ-30	Durante la investigación, la solución deberá contar con un motor analítico responsable de la reconstrucción de la cadena de causalidad para determinar rápidamente todos los procesos involucrados en el incidente.
REQ-31	En el caso de producirse algún incidente de seguridad, la solución deberá proporcionar acciones de respuesta y remediación que se aplicarán sobre la red y/o los endpoints tales como: • Terminación de un proceso. • Eliminación o poner en cuarentena un fichero. • Ejecución de scripts. • Aislamiento de equipos infectados en la red. • Acceso a los ficheros de forma remota mediante la descarga o subida por parte del analista. • Ejecución de comandos y código interactivamente en cualquier equipo utilizando scripts de python o CMD. • Creación de IOCs basados en el comportamiento para la generación de nuevas alertas. • Blacklisting/Whitelisting. • Remediación.
REQ-32	La consola de gestión deberá poder proporcionar al analista al menos la siguiente información:

	• Visor de eventos con prioridad. • Cadena de actividad/causalidad. • Timeline del ataque. • Visualización de la actividad y contexto para la investigación y detección de ataques. • Dashboard de Incidentes y gravedad incluyendo la asignación de incidentes por parte de los analistas, bloc de notas y panel de discusión. Consultas personalizadas sobre los datos durante una investigación, incluyendo búsquedas de IOCs. • Integración con herramienta de Inteligencia de amenazas que enriquezca la información de contexto de los incidentes aportando información útil para su análisis.
Ref.	Cortex XDR PRO o equivalente (500 licencias + 100 licencias adicionales).

I.5. Versiones soportadas

La solución XDR deberá cumplir los siguientes requisitos:

Requisito	**Descripción**

REQ-33	La solución deberá ser compatible con las siguientes versiones de Windows, Mac, Linux y Android:
	• Windows
	  ○ Windows XP 32bit SP3 o superior
	  ○ Windows Vista SP1 y superior
	  ○ Windows 7 RTM y 7 SP1
	  ○ Windows Embedded Standard 7 y 7 SP1
	  ○ Windows Embedded POSReady 7 y 2009
	  ○ Windows 8.1 y 8.1 FIPS
	  ○ Windows Embedded Professional 8.1
	  ○ Windows 10 Education, 10 Pro, 10 Enterprise, 10 1709, 10 1803, 10 1809, 10 RS6 1903, 10 1909, 10 2004, 10 20H2, 10 21H1
	  ○ Windows 10 Enterprise 2019 LTSC
	  ○ Windows Server Datacenter
	  ○ Windows Server 2003 32 bit SP2 o superior, 2008, 2008 R2 SP1, 2012, 2012 R2, 2016, 2016 Datacenter Edition, Core Option (2021, 2012 R2, 2016), 2019 (Server Core)

	• Mac (intel y ARM M1)
	  ○ MacOS 10.11 o superior
	• Linux
	  ○ Amazon Linux 2 LTS Candidate 1 y 2.
	  ○ Amazon Linux AMI 2017.03, 2017.09, 2018.03
	  ○ Azure Virtual Desktop (WVD o AVD)
	  ○ CentOS 6 o superior
	  ○ Debian 8 o superior
	  ○ Oracle 6 o superior.
	  ○ Red Hat Enterprise Linux 6 o superior
	  ○ OpenSuse Leap 15.1
	  ○ SUSE Linux Enterprise Server 11 SP4, 12, 15 SP0, 15 SP1, 15 SP2
	  ○ Ubuntu Server 12 o superior
	• Virtual Applications
	  ○ Citrix Virtual Apps and Desktops 7.13 o superior
	  ○ Citrix App Layering 4 o superior
	  ○ VMware AppVolumes 2.12.1 o superior
	  ○ VMware Horizon View 7.1 o superior
	  ○ VMware ThinApp 5.2.2 o superior
	• Android 5, 6, 7, 8, 9 y 10
	• Kubernetes Cloud
	  ○ GCP- GCOS, Ubuntu
	  ○ Azure - ubuntu 18
	  ○ AWS - Amazon Linux 2, Ubutu 18/20, RHEL 7/8

Ref.	Cortex XDR PRO o equivalente (500 licencias + 100 licencias adicionales).

I.6. Servicio de soporte Premium

El servicio de soporte Premium deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-33	Soporte telefónico 24x7.
REQ-34	Orientación y supervisión para ayudar a acelerar la instalación y configuración inicial a medida que se implante la solución XDR en la APB.

REQ-35	Transferencia de conocimientos clave y opciones de capacitación para aprovechar al máximo la solución XDR. • Acceso a la comunidad. • Acceso a la base de conocimientos y documentación en línea. • Acceso a la formación en línea.
REQ-36	Asesoramiento continuado y personalizado para garantizar la planificación de la estrategia de protección en materia de ciberseguridad. • Guía de mejores prácticas. • Revisión de nuevas funcionalidades y releases. • Health check anual.
REQ-37	Excelencia operativa, ayudando a integrar la solución XDR con flujos de trabajo operativos para garantizar una alineación perfecta con la red e infraestructura de seguridad de la APB. • Monitorización proactiva del uso. • Revisiones operativas periódicas. • Revisiones ejecutivas de negocio.
REQ-38	Soporte técnico con acceso a expertos técnicos y recursos en línea de manera ilimitada para garantizar que el negocio de la APB esté protegido. • Acceso al portal de atención al cliente. • Soporte telefónico 24x7.

I.4. Hosting Insights

Con la información de Host Insights es posible tener visibilidad completa e inventariado de los datos operativos y de negocio de TI. Al contar con un inventario único en un solo lugar, se podrán identificar rápidamente problemas de seguridad existentes en la APB.

El servicio de Hosting Insights deberá cumplir los siguientes requisitos:

Requisito	**Descripción**

REQ-39	Información del endpoint
	Para cada endpoint, la solución XDR deberá enumerar todos los detalles sobre el mismo, incluyendo:
	• Datos del usuario.
	  ○ Detalles identificativos sobre el usuario, como nombre y SID.
	• Grupos.
	  ○ Detalles sobre la cuenta como:

	▪ Si es una cuenta activa. ▪ El tipo de cuenta: • Cuenta duplicada temporal. • Cuenta normal. • Cuenta de confianza entre dominios. • Cuenta de confianza de la estación de trabajo. • Cuenta de confianza del servidor. • Usuarios a grupos. o Información sobre la contraseña establecida para esta cuenta de usuario: si se requiere una contraseña para iniciar sesión, si la contraseña se puede cambiar y si la contraseña tiene una fecha de vencimiento. • Información de grupos. • Mapeo de usuarios y grupos. • Servicios. • Drivers. • Autoarranque. • Sistema (Hardware y Software). • Recursos compartidos. • Discos.
REQ-40	Inventario de Host y Vulnerabilidades Existentes La solución XDR deberá gestionar las vulnerabilidades, identificando y cuantificando las vulnerabilidades de seguridad de las aplicaciones instaladas en los endpoints de la APB. Asimismo, la solución XDR proporcionará un inventario que indique aplicaciones y versiones, así como detecte la presencia de vulnerabilidades, indicando CVE y riesgo, para ayudar en el análisis y priorización.
REQ-41	Search & Destroy Para tomar medidas inmediatas sobre archivos maliciosos conocidos y sospechosos, la solución XDR deberá permitir buscar y destruir los archivos desde la consola de administración. Se podrán buscar archivos específicos mediante SHA256 o una ruta con wildcards.
Ref.	Host Insights add-on Cortex XDR o equivalente (500 licencias + 100 licencias adicionales).

I.5. Servicio de Managed Threat Hunting

Es un servicio de hunting proactivo que aúna técnicas manuales, semiautomáticas y automáticas, con el objetivo de descubrir amenazas avanzadas dentro de la organización como ataques y campañas organizadas, cibercriminales, usuarios internos maliciosos o malware. Sus principales características son:

- Detección y monitorización 24x7x365 sobre endpoints, red y nube.
- Threat hunting por expertos del fabricante.
- Inteligencia integrada con Autofocus.
- Acceso a analíticas de comportamiento y reglas especiales del servicio.
- Reportes de amenazas describiendo incidentes de seguridad críticos.
- Reportes de impacto indicando amenazas emergentes y la exposición del cliente.
- Reportes de cyber higiene.
- Reporte mensual con un resumen del servicio.
- Integración dentro de la propia consola de la solución XDR.
- Asistencia directa e interactiva por parte del equipo de Managed Threat Hunting, que actúa como un equipo extendido de seguridad de la organización.

El servicio de Managed Threat Hunting deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-42	Monitorización y detección proactiva gestionada por parte del fabricante 24x7, a lo largo de datos XDR integrados (al menos endpoint, red y nube).
REQ-43	Incorporación de fuentes de inteligencia propias, analíticas de comportamiento y reglas de detección.
REQ-44	Investigación para comprender la amenaza: causa raíz, análisis de impacto, plan de acción, etc.
REQ-45	El servicio deberá notificar a la APB sobre la amenaza, con todos los detalles relevantes y los siguientes pasos recomendados.
REQ-46	El equipo de Threat Hunting revisará todos los datos recopilados en la base de datos de logs integral (endpoint, red y nube).
REQ-47	Reportes de amenazas describiendo los incidentes de seguridad críticos detectados.
REQ-48	Reportes de impacto revelando amenazas emergentes y la exposición del cliente.
REQ-49	Integrado en la consola de la solución XDR para la gestión de incidentes.

REQ-50	Comunicación bidireccional con los analistas asignados, tanto a través la consola XDR como a través de correo electrónico.