

Expediente P.O.123.24

Pliego de Prescripciones Técnicas para la contratación de la Asistencia Técnica - Administrador de Seguridad (AS) para el soporte técnico en el cumplimiento del ENS en la Autoridad Portuaria de Baleares.



## Índice

Índice .....	2
1 Antecedentes y justificación.....	4
2 Objeto del contrato .....	4
3 Documentación a disposición de la empresa adjudicataria.....	5
4 Legislación y normas que regirán los trabajos a realizar .....	5
5 Descripción de las tareas objeto del contrato .....	7
5.1.1 Gestión del proyecto .....	7
5.1.2 Desarrollo de las tareas del Administrador de Seguridad (AS).....	7
5.1.3 Horario y lugar de prestación del servicio.....	11
6 Entregables .....	12
7 Acuerdos de nivel de servicio .....	13
7.1.1 ANS de gestión de la documentación .....	13
7.1.2 ANS del equipo de trabajo .....	14
7.2 Penalizaciones.....	15
8 Calendario previsto .....	15
9 Medios personales mínimos .....	16
10 Requisitos técnicos .....	18
11 Presupuesto .....	19
12 Seguridad.....	20
12.1 Acceso a los sistemas de la APB .....	20
12.2 Cambios de la empresa.....	20
12.3 Incidentes de seguridad de la información.....	21
12.4 Confidencialidad de la información.....	21
12.5 Derecho de auditoría.....	22
12.6 Requisitos de seguridad en caso de subcontratación .....	22
12.7 Servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la APB.....	22
12.8 Conformidad de sistemas, productos y equipos.....	22
13 Informes sobre el desarrollo de los trabajos .....	23
14 Defectos o deficiencias de los trabajos.....	23
15 Contradicciones y omisiones del presente documento .....	23
16 Consideración final.....	23





# Ports de Balears



Autoritat Portuària de Balears

Anexo I. Medios personales a adscribir .....	25
Anexo II. Solvencia técnica de la empresa .....	29
Anexo III. Justificación de precios.....	30





## 1 Antecedentes y justificación

La Autoridad Portuaria de Baleares (APB, en adelante) está en pleno proceso de la certificación de conformidad con el Esquema Nacional de Seguridad (ENS) (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad) en sus sistemas de información.

En el momento de la redacción del presente Pliego la APB ha efectuado una auditoría interna para conocer el grado de conformidad con el ENS y las medidas de aplicación para la protección de datos de carácter personal según se recoge en el RGPD y la LOPDGDD.

Uno de los próximos objetivos estratégicos de la APB es garantizar la adecuación, el mantenimiento y la mejora continua de la seguridad de sus sistemas de información cumpliendo con la normativa de obligado cumplimiento del ENS, NIS2 así como el Reglamento de Protección de Datos (RGPD), de modo que se permita reforzar la confianza de la ciudadanía y las empresas en la relación electrónica con la APB, mejorando la calidad y seguridad de los servicios ofrecidos.

Por otro lado, la APB está adherida al contrato E/062/21 “*Servicio de Ciberseguridad para Puertos del Estado y Autoridades Portuarias*”, liderado por Puertos del Estado, desde el cual se ofrecen servicios de adecuación al ENS. Este contrato contempla entre otros objetivos, la elaboración de un plan de adecuación al ENS o la adaptación del existente con el objetivo de obtener la certificación en el ENS. Tras la finalización de la fase inicial de certificación, se incluyen acciones necesarias para obtener el sello de conformidad de otros sistemas de información así como optimizar los existentes (ciclo de mejora continua), así como la realización de una revisión anual del análisis de riesgos de los sistemas de información dentro del alcance del ENS. Además, con este contrato se ofrece a la APB los servicios de un SOC.

Por este motivo, resulta imprescindible contar con un soporte técnico especializado que permita a la APB avanzar en el cumplimiento normativo, asegurar la correcta implementación de las medidas del ENS, las de la legislación NIS2, supervisión de los servicios del SOC y fortalecer su sistema de gestión de la seguridad de la información. Este contrato se enmarca en la necesidad de disponer de recursos y capacidades que garanticen la alineación con los estándares exigidos y con el contrato de Puertos del Estado, contribuyendo al logro de los objetivos estratégicos en materia de seguridad y protección de datos.

## 2 Objeto del contrato

El objeto de este contrato es la contratación de la Asistencia Técnica para desempeñar el rol de Administrador de Seguridad (AS) según funciones definidas en la [Guía de Seguridad de las TIC \(CCN-STIC-801\) Esquema Nacional de Seguridad - Responsabilidades y Funciones](#), así como asistencia al Responsable de Seguridad en la supervisión y coordinación del SOC de la APB, asistencia en el Plan de formación y concienciación en seguridad de la información de la APB y asistencia en la adecuación de los sistemas de información al ENS y NIS2, así como cumplimiento de resto normativa vigente aplicable en materia de ciberseguridad y protección de datos personales. El servicio del Administrador de Seguridad se prestará exclusivamente de manera presencial en las instalaciones de la APB con una dedicación del 100%.





La empresa adjudicataria deberá desarrollar durante la vigencia del contrato, y bajo las directrices del Responsable de Contrato, las tareas y servicios que se detallan en el apartado 5 de este Pliego, garantizando el soporte técnico necesario durante todo el período de vigencia del presente contrato.

### 3 Documentación a disposición de la empresa adjudicataria

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 de uso oficial 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 expediente 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.
- **Interoperabilidad**
  - Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
  - Normas Técnicas de Interoperabilidad derivadas del Esquema Nacional de Interoperabilidad.
- **Identificación y firma electrónica**
  - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- **Seguridad y protección de datos**
  - Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de





diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2).

- 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.
- 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.
- **Accesibilidad**
  - Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
  - Directiva (UE) 2016/2102, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público
  - Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- 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.

También se tendrá en cuenta para realizar los trabajos la adecuación a las certificaciones ISO-9001, ISO-14001 e ISO-30301 que posee la APB.



## 5 Descripción de las tareas objeto del contrato

Con carácter enunciativo y no exhaustivo, se relacionan las siguientes tareas que tendrán que ser realizadas por la empresa adjudicataria del contrato.

### 5.1.1 Gestión del proyecto

La empresa adjudicataria dispondrá de un Jefe/a del Proyecto para la gestión del contrato. La metodología a utilizar estará basada en el marco de gestión de proyectos PMBOK, siguiendo las directrices marcadas por el Responsable del Contrato. Para ello, desde el punto de vista de la gestión de proyectos se van a establecer tres (3) fases de gestión:

- a) **Fase de gestión inicial.** Se iniciará formalmente el proyecto y se adaptará y validará el plan de trabajo a seguir.
- b) **Fase de gestión de ejecución.** Se ejecutarán los trabajos planificados, se realizará un seguimiento y control exhaustivo de dichos trabajos y, si es necesario, se modificará la planificación para adaptarse a las circunstancias.
- c) **Fase de gestión de finalización.** Se cerrará formalmente el proyecto, entregando toda la documentación pertinente tanto de gestión como de producto.

En cada una de estas fases se tendrán en cuenta las áreas de conocimiento de PMBOK que se consideren necesarias y se establezcan en la fase de iniciación.

La empresa adjudicataria deberá incluir una propuesta de metodología a seguir y especificar toda la documentación a entregar asociada a los grupos de procesos y áreas de conocimiento que establezca PMBOK que se deberá adaptar a las plantillas (si las hubiera) y procedimientos que determine el Responsable del Contrato.

La empresa adjudicataria está comprometida a garantizar la calidad del servicio, a cumplir los Acuerdos de Nivel de Servicio (ANS) definidos en el apartado 7 de este Pliego y a documentar e informar de su cumplimiento o incumplimiento a la APB. El incumplimiento de los ANS podrá originar penalizaciones.

### 5.1.2 Desarrollo de las tareas del Administrador de Seguridad (AS)

El Administrador de Seguridad (AS) es una figura clave en la gestión de la seguridad de los sistemas de información. El Administrador de Seguridad es responsable de implementar y supervisar las medidas de seguridad técnicas y operativas necesarias para proteger la información y garantizar la continuidad de los servicios.

La empresa adjudicataria aportará esta figura del Administrador de Seguridad, el cual deberá asumir y desarrollar las tareas, conforme a lo descrito en los apartados siguientes.

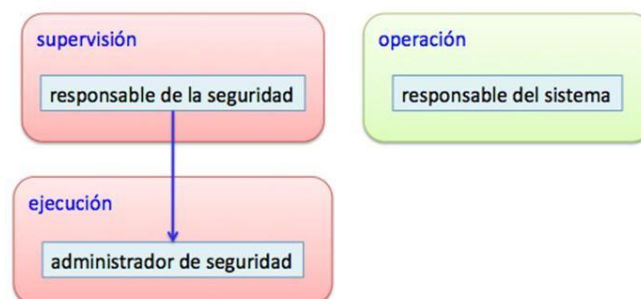
#### 5.1.2.1 Desarrollo de las funciones del Administrador de Seguridad (AS)

La empresa adjudicataria deberá asistir al Responsable Seguridad de la APB desarrollando, las funciones del Administrador de Seguridad definidas en la Guía de Seguridad de las TIC (CCN-STIC-801) Esquema Nacional de Seguridad - Responsabilidades y Funciones. En concreto:



- a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información de la APB.
- b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- c) La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- d) La redacción de la Normativa de Seguridad y la aplicación de los Procedimientos Operativos de Seguridad (POS).
- e) Asegurar que todos los controles de seguridad implementados sean rigurosamente observados y cumplidos.
- f) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- h) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- i) Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- k) Gestionar las relaciones con los proveedores y coordinar los servicios externalizados de la APB en materia de ciberseguridad.
- l) Desarrollar e implementar programas de formación y concienciación en la APB.
- m) Asistir a las reuniones de control y seguimiento periódicas que sean requeridas por el responsable de seguridad (RS).

El Administrador de Seguridad, bajo la dirección y supervisión del Responsable de Seguridad de la APB y en coordinación con el Delegado o Subdelegado de Protección de Datos (DPD), garantizará la operación de la ciberseguridad dentro de la APB.





## 5.1.2.2 Asistencia en las actividades del SOC y su coordinación

El Administrador de Seguridad asistirá al Responsable de Seguridad en diversas tareas relacionadas con los servicios proporcionados por el SOC de la APB (actualmente proporcionado por Puertos del Estado). Estas tareas, serán, como mínimo, las siguientes:

### a) Gestión de eventos e incidentes de seguridad

Proporcionando apoyo y los conocimientos técnicos necesarios en las siguientes actividades:

- **Actividad de monitorización de servicios y sistemas:** monitorización de servicios y sistemas para coordinar la identificación de posibles amenazas de seguridad en tiempo y forma.
  - **Protocolo de respuesta a incidencias:** supervisión y actualización los protocolos de respuesta a incidentes, asegurando una actuación rápida y eficiente en situaciones de emergencia, en coordinación con el SOC.
  - **Notificación de incidentes:** gestión de la notificación de incidentes a todas las partes interesadas internas y externas, incluyendo reguladores y otras entidades según sea necesario
- b) **Servicios de alerta temprana:** atención a las alarmas recibidas del sistema de alerta temprana del SOC, para identificar y comunicar potenciales amenazas de seguridad a la APB de manera proactiva.
- c) **Servicio de detección, análisis y gestión de vulnerabilidades:** supervisión de las evaluaciones regulares de vulnerabilidades realizadas por el SOC para identificar y remediar posibles debilidades en los sistemas de información.
- d) **Gestión de crisis y desastres:** supervisión, mantenimiento y mejora del plan de gestión de crisis y desastres de la APB, coordinando los esfuerzos de recuperación y continuidad del negocio en caso de un incidente mayor, asistiendo al Responsable de Seguridad (RS) de la APB y en coordinación con el SOC.
- e) **Vigilancia digital:** supervisión las operaciones de vigilancia digital realizadas por el SOC con el objeto de proteger los activos de información de la APB contra amenazas de ciberseguridad y posibles vectores de ataque.
- f) **Plan Director de Seguridad y asesoramiento:** asistencia al Responsable de Seguridad en la supervisión y actualización del Plan Director de Seguridad.
- g) **Gobierno de la seguridad (GRC y reporting):** asistencia al Responsable de Seguridad en la supervisión y gestión de las actividades relacionadas con la gobernanza, el riesgo y el cumplimiento (GRC).

### h) Coordinación con el SOC de la APB

La empresa asistirá al Responsable de Seguridad en la coordinación con el SOC de la APB, en concreto:

- **Comunicación:** asistencia en las comunicaciones con el SOC, reuniones y el intercambio de información de manera periódica.





- **Integración de normativas, políticas y procedimientos:** El Administrador de Seguridad (AS) asegurará que las actividades y tareas desarrolladas por el SOC están alineadas con las normativas, políticas y procedimientos de seguridad de la información de la APB.
- **Colaboración en la mejora continua:** El Administrador de Seguridad trabajará junto al SOC de la APB para revisar y mejorar continuamente las estrategias de seguridad de la información basadas en análisis de riesgo y evaluación de la efectividad de las medidas de seguridad implementadas.

### 5.1.2.3 Servicio de adecuación, seguimiento y mejora del ENS y NIS2

El Administrador de Seguridad asistirá al Responsable de Seguridad en la adecuación, seguimiento y certificación de nuevos sistemas de información en el ENS y normativa NIS2, todo ello enmarcado en un ciclo de mejora continua de los sistemas de información ya certificados o adecuados. Se incluye la asistencia al Responsable de Seguridad en la elaboración de toda la documentación necesaria para el cumplimiento normativo del ENS y NIS2.

### 5.1.2.4 Plan de formación y concienciación en seguridad de la información

El Administrador de Seguridad asistirá al Responsable de Seguridad en la realización, seguimiento y mejora del Plan de formación y concienciación en seguridad de la información de la APB. Ello requiere de la realización de las siguientes tareas:

- **Evaluación del estado inicial:** Evaluación de los conocimientos y conceptos de seguridad de la información por parte del personal de la APB y de los comportamientos y hábitos del personal de la APB frente a situaciones de riesgo. La evaluación se puede realizar mediante cuestionarios o encuestas y la evaluación de comportamientos mediante simulaciones que consistan en poner al personal en situaciones de riesgo controlado, tales como ataques de phishing o pérdidas de USB con información importante, y evaluar su comportamiento.
- **Elaboración del Plan de concienciación:** Tras la evaluación inicial deberá elaborar un Plan anual que incluya, al menos, las siguientes acciones:
  - Difusión del Plan dentro de la organización.
  - Establecer objetivos factibles y medibles que puedan ser evaluados.
  - Planificar las acciones orientadas a cumplir los objetivos establecidos en el Plan.
- **Ejecución del Plan:** Tras la elaboración y aprobación del Plan por parte del Responsable del Contrato, se deberá llevar a cabo tanto las acciones de capacitación, concienciación y entrenamiento como las evaluaciones correspondientes. Incluirá:
  - Seguimiento y promoción de actividades de concienciación y formación específicas dirigidas al personal directivo de la APB (al menos 1 sesión anual de 1h).
  - Seguimiento y promoción de actividades de concienciación y formación al personal no directivo de la APB (al menos 2 sesiones anuales de 2h cada sesión).





- Seguimiento y promoción de actividades de formación específicas para el personal técnico del departamento de sistemas de información (al menos 1 sesión anual de 1h).
  - Asistencia al Responsable de Seguridad en la organización los cursos de formación de ciberseguridad que proponga.
  - Realización de píldoras formativas para incluir en las newsletters internas de la APB.
  - Realización de simulaciones de phishing, ransomware o cualquier técnica de ataque informático.
  - Exámenes/cuestionarios de evaluación de conocimientos.
  - Cualquier otra acción que estime oportuna la APB
  - Seguimiento de métricas de evaluación de las actividades de formación y concienciación
- **Mejora continua:** Al finalizar el Plan anual y en función de los resultados obtenidos en las evaluaciones se propondrá un proceso de mejora continua de los resultados obtenidos que servirá para la elaboración del Plan de la siguiente anualidad.

### 5.1.3 Horario y lugar de prestación del servicio

La prestación del servicio del Administrador de Seguridad se realizará durante todo el año con el mismo horario y en horario laboral (se establece el horario laboral en los días laborables en Palma en horario de 9:00 a 18:00). Todos los servicios se prestarán de forma presencial en las oficinas de la APB en Palma (Moll Vell nº5) y deberán cubrir la totalidad del horario. Cabe tener en cuenta que la APB cuenta con distintas sedes (Palma, Maó, Eivissa, Alcúdia y La Savina) y, por necesidades del servicio, se podrá desplazar el Administrador de Seguridad a alguna de las otras sedes de la APB, sin coste alguno para la APB.

El Jefe/a del Proyecto para la gestión del contrato prestará sus servicios de forma presencial en las oficinas de la APB en Palma (Moll Vell nº5) en las oficinas de la APB al menos un día a la semana.

Asimismo, cabe tener en cuenta que la APB dispone de distintas sedes (Palma, Maó, Eivissa, Alcúdia y La Savina), pudiendo ser necesario desplazarse ocasionalmente a alguna de estas sedes en función de las necesidades del proyecto

La APB notificará al Jefe/a del Proyecto de la empresa adjudicataria o bien directamente al Administrador de Seguridad tareas a realizar o incidencias del servicio, ya sea de forma verbal (mediante reuniones presenciales), telefónicamente o mediante correo electrónico

La empresa adjudicataria dispondrá de un teléfono disponible 24x7 mediante el cual se podrá contactar directamente con el Administrador de Seguridad en el caso que ocurra un incidente de seguridad de la información de nivel de peligrosidad medio o superior según establece la [Guía de Seguridad de las TIC \(CCN-STIC-817\) Esquema Nacional de Seguridad - Gestión de ciberincidentes](#). En este caso, no habría coste adicional al importe del contrato.



## 6 Entregables

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, si cabe, de la APB.

El coste de elaboración y/o actualización de la documentación generada en el proyecto, está incluida en la partida de gestión del mismo.

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

Como resultado de los trabajos realizados, la empresa adjudicataria deberá entregar como mínimo la documentación siguiente:

### 1. Gestión del proyecto

- i. Plan de gestión del proyecto.
- ii. Informes de seguimiento y actas de las reuniones de seguimiento.
- iii. Variaciones no sustanciales del proyecto (si surgieran durante la ejecución del mismo).
- iv. Informe de cierre de proyecto.

### 2. Desarrollo de las tareas del Administrador de Seguridad (AS)

#### 2.1. Desarrollo de las funciones del Administrador de Seguridad (AS)

- v. Documentación relativa al Plan de Adecuación y guía de implantación del ENS y NIS2.
- vi. Normativa, procedimientos, guías e instrucciones de seguridad.
- vii. Procedimientos Operativos de Seguridad (POC).
- viii. Informes de monitorización del estado de seguridad del sistema.
- ix. Informes mensuales de servicio:
  - a. Actividades realizadas, en curso y pendientes.
  - b. Registro de incidencias.
  - c. Registro de peticiones de cambios.
  - d. Seguimiento de ANS.
  - e. Documentación generada durante el mes en curso.

#### 2.2. Coordinación con el SOC de la APB

- x. Informes de reporting al Responsable de Seguridad (RS).
- xi. Informes mensuales de servicio:
  - a. Actividades realizadas, en curso y pendientes.
  - b. Registro de incidencias.
  - c. Registro de peticiones de cambios.
  - d. Seguimiento de ANS.
  - e. Documentación generada durante el mes en curso.



## 2.3. Plan de formación y concienciación en seguridad de la información

- xii. Plan de formación y concienciación en seguridad de la información.
- xiii. Informes de las acciones de formación y concienciación realizadas (sesiones, asistentes, contenido, incidencias...).
- xiv. Documentación utilizada para realizar las acciones de formación y concienciación.

## 7 Acuerdos de nivel de servicio

La prestación de los servicios objeto de este Pliego estarán sujetos, en la medida de lo posible, a acuerdos de nivel de servicio (ANS) con posibles 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.

La empresa adjudicataria utilizará la herramienta de gestión de incidencias (JIRA) que la APB dispone, de modo que se permita conocer, con una antelación razonable, las posibles incidencias que puedan afectar a la correcta prestación de los servicios, de tal manera que sea posible identificar las situaciones de riesgo de incumplimiento de las condiciones de prestación de servicios y aplicar así las medidas correctoras oportunas.

Adicionalmente, la empresa adjudicataria, deberá proveer a la APB un cuadro de mando que permita consultar en tipo real los ANS requeridos y su cumplimiento

A continuación, se definen los ANS que establecerán los umbrales mínimos de calidad exigidos en la prestación de los servicios definidos en el apartado 5 de este Pliego.

### 7.1.1 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 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
DOC.01	Control de la documentación = (Número de documentos no actualizados o inexistentes, detectados / Número de documentos auditados) x 100	100 % (periodicidad de medida mensual)

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
DOC.02	Número de documentos entregados fuera de plazo	0 (periodicidad de medida mensual)

## 7.1.2 ANS del equipo de trabajo

El equipo de trabajo que la empresa adjudicataria determine en su oferta y que deberá incluir como mínimo los perfiles indicados en el apartado 9 de este Pliego, estará sujeto a la aplicación de los siguientes indicadores:

### 1. Incorporación de los recursos propuestos del equipo de trabajo el primer día de contrato.

Código	Cálculo	Valor Máximo Objetivo
EQT.01	Desviación en días desde el primer día laborable de contrato hasta la incorporación efectiva del recurso	0 días laborables

### 2. Coberturas de los recursos propuestos del equipo de trabajo.

Código	Cálculo	Valor Máximo Objetivo
EQT.02	Días transcurridos con menos recursos que los propuestos por oferta, durante el periodo de facturación	0 días laborables

### 3. Notificación de salida de los recursos propuestos del equipo de trabajo.

Código	Cálculo	Valor Máximo Objetivo
EQT.03	Diferencia de días en la comunicación de la salida de un recurso, incumpliendo el período de preaviso fijado en este Pliego, durante el período de facturación	0 días laborables

### 4. Período de solapamiento entre recursos propuestos del equipo de trabajo.

Código	Cálculo	Valor Máximo Objetivo
--------	---------	-----------------------



EQT.04	Número de días de incumplimiento en el período de solapamiento entre un recurso saliente y el entrante, durante el periodo de facturación	0 días laborables
--------	---	-------------------

### 5. Nivel de rotación de los recursos propuestos del equipo de trabajo.

Código	Cálculo	Valor Máximo Objetivo
EQT.05	Número de cambios no solicitados de los recursos propuestos, a lo largo de un año. No computan las coberturas siempre y cuando se hagan con los mismos suplentes	1 cambio/año

## 7.2 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.

La empresa adjudicataria entregará un informe detallando los niveles de servicio del mes anterior antes del décimo día laborable de cada mes.

La APB realizará una revisión mensual del cumplimiento de los niveles de servicio establecidos. En caso de que no se cumplan estos niveles de servicio, la APB podrá proceder a la aplicación de las penalizaciones indicadas en el Cuadro de Características del Pliego Administrativo.

La aplicación de estas sanciones no exime a la empresa adjudicataria de la obligación de cumplir con sus compromisos contractuales, ni limita el derecho de la APB a reclamar una compensación por daños y perjuicios que pudieran surgir.

## 8 Calendario previsto

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

Independientemente del calendario propuesto en la propuesta técnica, el calendario final se deberá consensuar y aprobar por parte del Responsable del Contrato la APB.

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 siguiente planificación.

Actividades	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Gestión del proyecto												
Desarrollo de las tareas del Administrador de Seguridad (AS)												



## 9 Medios personales mínimos

La empresa adjudicataria se comprometerá a adscribir para este contrato, los medios personales mínimos recogidos en este apartado.

El equipo humano que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por las personas propuestas por los licitadores en las ofertas presentadas.

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.

El equipo de trabajo estará formado, como mínimo, por los siguientes perfiles que se detallan a continuación:

### Perfil 1: Jefe/a de proyecto

#### A. Funciones:

- Realizar la dirección, seguimiento y control del proyecto, según lo definido en el apartado 5.1.1 *Gestión del Proyecto*
- Generar la documentación de control del proyecto.
- Revisar los trabajos y la documentación realizada por el equipo de trabajo.
- Garantizar la calidad del producto final.
- Participar en la elaboración y realización de presentaciones divulgativas del proyecto.
- Llevar a cabo la interlocución con la APB, como representante de la empresa adjudicataria, a todos los efectos.
- Colaborar directamente en la dirección de los trabajos en estrecha relación con el responsable de los mismos.
- Estructurar el funcionamiento y las tareas del equipo de trabajo.
- Organizar las relaciones del equipo de trabajo.
- Analizar los informes de seguimiento de los trabajos y recomendar acciones preventivas y correctivas.
- Realizar la coordinación y asistencia a la dirección en las reuniones de seguimiento general de los trabajos.

#### B. Dedicación parcial presencial en las oficinas de la APB de Palma, de al menos 1 día a la semana.

#### C. Requisitos mínimos:

- Titulación universitaria nivel MECES 3 (Máster) en estudios relacionados con las TIC (informática/telecomunicaciones).
- Cinco (5) años de experiencia dirigiendo proyectos de seguridad de la información y protección de datos para la Administración Pública





- Formación específica en Dirección y Gestión de Proyectos.
- Disponer de la certificación vigente PMP (Project Management Professional) de PMI.
- Disponer de al menos de una (1) de las siguientes certificaciones oficiales en el ámbito de seguridad de la información:
  - CISM (Certified Information Security Manager) de ISACA.
  - CISSP (Certified Information Systems Security Professional) de ISC2.
  - Lead Auditor 27001.

## Perfil 2: Consultor experto en ciberseguridad

### A. Funciones:

- Desarrollar las tareas definidas en el apartado *5.1.2 Desarrollo de las tareas del Administrador de Seguridad (AS)*

### B. Dedicación presencial 100% en las oficinas de la APB de Palma

### C. Requisitos mínimos:

- Titulación universitaria nivel MECES 3 (Máster) en estudios relacionados con las TIC (informática/telecomunicaciones).
- Diez (10) años de experiencia en proyectos de seguridad de la información y protección de datos para la Administración Pública.
- Participación en al menos un (1) proyecto de implantación del ENS.
- Disponer de al menos de dos (2) de las siguientes certificaciones oficiales en el ámbito de seguridad de la información:
  - CISA (Certified Information System Auditor) de ISACA.
  - CISM (Certified Information Security Manager) de ISACA.
  - CISSP (Certified Information Systems Security Professional) de ISC2.
  - Lead Auditor 27001.
  - Lead Implementer 27001.
  - Lead Auditor 22301.

Las empresas licitadoras podrán incluir otros perfiles adicionales para la realización de las tareas específicas que crean conveniente y, en todo caso, incluyéndolos en la planificación.

### **Cumplimiento de los requisitos exigidos en materia de titulación:**

Para el cumplimiento de los requisitos exigidos en materia de titulación en el presente pliego, se tomará como referencia el **Marco Español de Cualificaciones para la Educación Superior (MECES) el catálogo de Títulos Universitarios “Pre-Bolonia y el Marco Europeo de Cualificaciones (EQF -European Qualifications Framework):**

- Titulación de Máster: MECES nivel 3 (equivalente a EQF nivel 7). Titulación oficial académica de Máster Universitario, Licenciado o Ingeniero.



- Titulación de Grado: MECES nivel 2 (equivalente a EQF nivel 6). Titulación oficial académica de Grado, Diplomado Universitario o Ingeniero Técnico.
- Titulación de Técnico Superior en Formación Profesional: MECES nivel 1 (equivalente a EQF nivel 6). Titulación oficial académica de ciclo formativo de técnico superior o equivalente.

A los efectos del cumplimiento de los requisitos exigidos como adscripción de medios cada nivel MECES engloba a todos los niveles inferiores, por lo que se aceptará cumplido el requisito de titulación cuando se presente una titulación igual o superior a la requerida.

En caso de que la titulación presentada en estos roles no esté relacionada con las áreas especificadas en la descripción de cada perfil, el rol podrá ser rechazado a excepción de aquellos perfiles que indique expresamente que se requiere otra titulación.

A efectos informativos se identifican las titulaciones exigidas en cada perfil:

- (1) Antes de Bolonia: Ingeniería superior en Informática o Telecomunicaciones. Después de Bolonia: Grado en Informática o Telecomunicaciones + Máster Universitario que habilite para ejercer la profesión de Ingeniero informático o de Telecomunicaciones. NIVEL MECES: 3
- (2) Antes de Bolonia: Ingeniería Técnica o Diplomatura en Tecnologías de la Información Después de Bolonia: Grado en tecnologías de la Información. NIVEL MECES: 2
- (3) Antes de Bolonia: Diplomatura en el ámbito de la información y documentación Después de Bolonia: Grado en el ámbito de la información y documentación. NIVEL MECES: 2
- (4) Estudios de Formación Profesional II de Técnico Especialista o estudios de Ciclo Superior de Formación Profesional en el ámbito de la Información y las Comunicaciones. NIVEL MECES: 1
- (5) Antes de Bolonia: Ingeniería Técnica o Diplomatura en Tecnologías de la Información periodismo o comunicación audiovisual. Después de Bolonia: Grado en tecnologías de la Información. NIVEL MECES: 2
- (6) Antes de Bolonia: Diplomatura, Ingeniería Técnica en el ámbito de las Tecnologías de la Información, Ciencias Jurídicas o Administración y Dirección de empresas. Después de Bolonia: Grado en el ámbito de las Tecnologías de la Información, Ciencias Jurídicas o Administración y Dirección de empresas. NIVEL MECES: 2
- (7) Estudios de Formación Profesional de segundo grado de Técnico Especialista o Ciclo Formativo de Grado Superior de Formación Profesional en el ámbito de la Información y las comunicaciones o de la gestión y administración de empresas. NIVEL MECES: 1

## 10 Requisitos técnicos

Los requisitos técnicos exigidos en esta contratación son:

- La empresa licitadora deberá estar en posesión de los siguientes certificados (en vigor):

Pliego de Prescripciones Técnicas para la contratación de la Asistencia Técnica - Administrador de Seguridad (AS) para el soporte técnico en el cumplimiento del ENS en la Autoridad Portuaria de Balears (P.O.123.24).





- Esquema Nacional de Seguridad (ENS) nivel MEDIO, en los sistemas de información que soportan los servicios de consultoría en seguridad de la información y/o ciberseguridad

Esta exigencia se extenderá también a la **cadena de suministro** de dichos contratistas (en especial, a los subcontratistas), en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos. Las Certificaciones de Conformidad con el ENS, se ajustarán a la Instrucción Técnica de Seguridad aprobada por la Secretaria de Estado de Administraciones Públicas, y deberán mantenerse en vigor durante toda la ejecución del contrato.

## 11 Presupuesto

El **Presupuesto Base de Licitación** correspondiente a la primera anualidad (período inicial del contrato) asciende a la cantidad de **CIENTO SETENTA Y TRES MIL TRESCIENTOS VEINTINUEVE EUROS CON TREINA Y CUATRO CÉNTIMOS (173.329,34 €)** de los que **TRENTA MIL OCHENTA Y UN EUROS CON NOVENTA Y CINCO CÉNTIMOS (30.081,95 €)** corresponden al 21% de IVA

El **Valor Estimado del Contrato** (período inicial más las tres posibles prórrogas), asciende a la cantidad de **SEISCIENTOS NOVENTA Y TRES MIL TRESCIENTOS DIECISIETE EUROS CON TREINTA Y SIETE CÉNTIMOS (693.317,37 €)** de los que **CIENTO VEINTE MIL TRESCIENTOS VEINTISIETE EUROS CON OCHENTA Y UN CÉNTIMOS (120.327,81 €)** corresponden al 21% de IVA y **QUINIENTOS SESENTA Y DOS MIL NOVECIENTOS OCHENTA Y NUEVE EUROS CON CINCUENTA Y SEIS CÉNTIMOS (572.989,56 €)** al importe sin IVA.

Presupuesto			
Partida	Meses	Precio/mes	Total
<b>CAP. 1. GESTIÓN DEL PROYECTO</b>			
1.1. Gestión del proyecto	12	1.440,00 €	17.280,00 €
<b>CAP. 2. DESARROLLO DE LAS FUNCIONES DEL ADMINISTRADOR DE SEGURIDAD (AS)</b>			
2.1. Desarrollo de las funciones del Administrador de Seguridad (AS)	12	8.591,33 €	103.095,96 €
<b>PRESUPUESTO</b>			<b>120.375,96 €</b>
BI (6%) + GG (13%)			22.871,43 €
<b>IMPORTE LICITACION (IVA excluido): PRESUPUESTO + BI Y GG (1 AÑO)</b>			<b>143.247,39 €</b>
IVA (21%)			30.081,95 €
<b>PRESUPUESTO BASE DE LICITACIÓN (1 AÑO)</b>			<b>173.329,34 €</b>
TOTAL PRIMERA PRÓRROGA (IVA excluido)			143.247,39 €
TOTAL SEGUNDA PRÓRROGA (IVA excluido)			143.247,39 €
TOTAL TERCERA PRÓRROGA (IVA excluido)			143.247,39 €
<b>TOTAL DE LAS PRÓRROGAS (1 AÑO + 1 AÑO + 1 AÑO) (IVA excluido)</b>			<b>429.742,17 €</b>
<b>IMPORTE ESTIMADO CONTRATO (1 AÑO + 1 AÑO + 1 AÑO + 1 AÑO) (IVA excluido)</b>			<b>572.989,56 €</b>
IVA (21%)			120.327,81 €
<b>IMPORTE TOTAL ESTIMADO CONTRATO IVA INCL:</b>			<b>693.317,37 €</b>



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 incluyen todos los costes laborales, ajustándose al Convenio Colectivo vigente. También está incluido en el coste de cada servicio el coste de elaboración de los entregables correspondientes solicitados en esta licitación.

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 cualquier otro gasto para el desarrollo de los mismos, están incluidos en los costes indicados de los servicios..

## 12 Seguridad

### 12.1 Acceso a los sistemas de la APB

La APB pondrá a disposición del adjudicatario los medios necesarios para realizar la conexión de uno o varios equipos informáticos a su red, con el fin de cumplir con lo especificado en este pliego. Será a criterio de la APB, previa consulta con el adjudicatario, la definición última de las características y capacidad de la conexión, que podrá ser mediante usuarios de acceso remoto (VPN-SSL) y/o poniendo a disposición en la sede del adjudicatario un punto de red para la interconexión. El adjudicatario podrá disponer, si así lo decide, de un cortafuegos en este punto, en cuyo caso será necesaria la adaptación y coordinación con la infraestructura y técnicos de la APB. En todo caso será necesario definir y restringir los accesos desde los dispositivos del adjudicatario a la red de la APB para su implementación en los cortafuegos corporativos.

La empresa adjudicataria deberá identificar a todos y cada uno de sus empleados que necesite conectarse a los sistemas de información de la APB 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.

### 12.2 Cambios de la empresa

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.



## 12.3 Incidentes de seguridad de la información

La empresa adjudicataria, se compromete a implementar y mantener un sistema robusto y efectivo de gestión de incidentes de seguridad para los servicios proporcionados a la APB, de acuerdo con los principios y requisitos establecidos por el ENS.

- **Notificación de incidentes:** La empresa adjudicataria notificará a la APB de manera inmediata y sin demora injustificada después de haber tomado conocimiento de cualquier incidente de seguridad que pueda afectar a los servicios objeto de este contrato.
- **Investigación y corrección:** La empresa adjudicataria se compromete a investigar de manera inmediata todos los incidentes de seguridad, a tomar las medidas correctivas necesarias para resolver el incidente y a mitigar su impacto. Además, cooperará con la APB en todas las etapas de la investigación y corrección.
- **Reportes de incidentes:** La empresa adjudicataria proporcionará a la APB informes regulares sobre la naturaleza y el estado de cualquier incidente de seguridad, incluyendo los detalles de las medidas correctivas tomadas y las recomendaciones para evitar incidentes similares en el futuro.
- **Cooperación con las autoridades:** Si el incidente de seguridad implica una violación de la ley, la empresa adjudicataria cooperará con las autoridades competentes y asistirá a la APB en el cumplimiento de sus obligaciones legales relacionadas con el incidente de seguridad.
- **Auditorías y pruebas:** La empresa adjudicataria permitirá y colaborará con las auditorías de seguridad y las pruebas de penetración que la APB pueda realizar o encargar, con el fin de evaluar la efectividad de las medidas de seguridad del Proveedor y su cumplimiento con esta cláusula y con el ENS.

En definitiva, el objetivo asegurar que cualquier incidente de seguridad en los servicios proporcionados a la APB se gestione de una manera que minimice los daños, preserve la confidencialidad, la integridad y la disponibilidad de la información, y cumpla con las obligaciones legales y reglamentarias.

## 12.4 Confidencialidad de la información

La APB considera que toda la información y documentación manejada durante el proyecto, del tipo que sea (electrónica, escrita o impresa, visual, verbal...), es estrictamente confidencial, por lo que cualquier vulneración de este principio que se observe será objeto de sanción de acuerdo a los términos establecidos en el apartado correspondiente de este pliego, incluso llegando a ser causa de resolución inmediata del contrato si así se estimara, todo ello sin perjuicio de las responsabilidades penales o de otro tipo a que hubiera lugar.

Toda la información y documentación que se maneje en el ámbito del presente contrato es propiedad de la APB. El adjudicatario se compromete a no difundir ni divulgar esta información, ni hacer uso alguno de ella más allá de las actividades vinculadas al contrato y que hayan sido expresamente autorizadas por escrito por la APB, así como a devolver la documentación que obre en su poder a la finalización del mismo, incluso aquella almacenada en



formato electrónico o por cualquier otro medio existente o futuro. Esta obligación ostentará el carácter de indefinida, desde el momento de la adjudicación de los trabajos.

El adjudicatario está obligado a comunicar a la APB la relación del personal de la organización implicado en el servicio, solicitando autorización previa para aquellos que deban hacer uso de esta información, así como informar de cualquier modificación en esta relación que pueda ocurrir durante el desarrollo del servicio.

Además de las anteriores obligaciones, el personal del adjudicatario está obligado a:

- Adaptarse a, y cumplir estrictamente, las normas internas de las APB en cuanto a políticas de seguridad, así como cualquier otra que sea de aplicación durante este proyecto.
- Mantener la información confidencial en estricta reserva y debidamente protegida mientras obre en su poder.
- Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización.
- Instruir al personal que estará encargado de recibir la información confidencial en el correcto uso de la misma y sus responsabilidades adquiridas.

### 12.5 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.

### 12.6 Requisitos de seguridad en caso de 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.

### 12.7 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.

### 12.8 Conformidad de sistemas, productos y equipos

La empresa adjudicataria utilizará 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.

### 13 Informes sobre el desarrollo de los trabajos

La empresa adjudicataria informará al Responsable del Contrato, con una periodicidad mínima mensual y en todo caso cada vez que le sea solicitado, y en la forma que el Responsable del Contrato considere oportuna en cada momento, sobre la marcha general de los trabajos encomendados.

Independientemente, en el Plan de Trabajos a concretar con fechas determinadas tras la adjudicación, se redactará el calendario de reuniones, a las que asistirá el Responsable del Contrato y el personal de su equipo que se estime oportuno, para el análisis del desarrollo de los trabajos. Se podrá requerir una (1) reunión presencial mensual.

El Responsable del Contrato podrá convocar periódicamente reuniones con la empresa adjudicataria para comprobar la calidad de los trabajos y el cumplimiento del Plan de Trabajos y del Pliego de Prescripciones Técnicas.

### 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 período 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 la



## Autoritat Portuària de Balears

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

Revisado y Conforme

**José Miguel Esteve Lledó**  
Responsable de Departamento de Desarrollo  
Tecnológico e Innovación  
VºBº

**Javier Segovia Mascaró**  
Jefe de Departamento de Desarrollo  
Tecnológico e Innovación  
VºBº

**Santiago Alejos Fernández**  
Subdirector

**Antonio Ginard López**  
Director



## Anexo I. Medios personales a adscribir

### SÓLO AL PROPUESTO COMO ADJUDICATARIO

#### **DATOS DEL PERFIL: Jefe/a de proyecto (perfil aplicable al objeto del contrato):**

Identificación oferta:	
Empresa licitadora:	
Perfil:	<b>Jefe/a de proyecto</b>
Nombre y apellidos:	

	Requisitos mínimos	
Titulación (MECES 3) en estudios relacionados con las TIC (informática/telecomunicaciones) :	Sí	- Rellenar Tabla 1 Titulaciones - La titulación deberá ser oficial, o en su defecto, reconocida por el Ministerio de Educación y Formación Profesional.
Experiencia mínima de 5 años dirigiendo proyectos en Administración Pública (años):	Sí	- Rellenar Tabla 2. Experiencia mínima en Administración Pública
Dedicación (número días a la semana de presencia en oficinas APB Palma): 1 día mínimo	Nº días:	
Formación específica en Dirección y Gestión de Proyectos	Sí	- Rellenar Tabla 3. Formación específica en Dirección de Proyectos
Titulación PMP de PMI	Sí	Fecha certificado:
Certificación oficial el ámbito de la seguridad de la información	Sí	- Rellenar Tabla 4. Certificaciones oficiales en el ámbito de la seguridad de la información

#### Tabla 1. Titulaciones académicas:

Código	Título académico	Nivel MECES	Duración	Centro	F-expedición
T1					dd/mm/aaaa
...					
Tn					

Duración: duración oficial.

#### Tabla 2. Experiencia mínima de 5 años en Administración Pública:

Empresa	Perfil ejercido en el proyecto	F-inicio	F-fin	Meses	Administración Pública
E1		dd/mm/aaaa	dd/mm/aaaa		
...					
En		dd/mm/aaaa	dd/mm/aaaa		

#### Tabla 3. Formación específica en Dirección de Proyectos:

Nº	Curso/Certificación	Horas	Entidad/Organismo	F-certificado
F1				
...				
Fn				





Tabla 4. Certificación oficial en el ámbito de la seguridad de la información:

Nº	Certificación	Entidad/Organismo	F-certificado
C1			
..			
Cn			

**DATOS DEL PERFIL: Consultor/a experto en ciberseguridad (perfil aplicable al objeto del contrato):**

Identificación oferta:	
Empresa licitadora:	
Perfil:	<b>Consultor/a experto en ciberseguridad</b>
Nombre y apellidos:	

	Requisitos mínimos	
Titulación (MECES 3) en estudios relacionados con las TIC (informática/telecomunicaciones) :	Sí	- Rellenar Tabla 1 Titulaciones - La titulación deberá ser oficial, o en su defecto, reconocida por el Ministerio de Educación y Formación Profesional.
Experiencia mínima de 10 años en proyectos de seguridad de la información y protección de datos para la Administración Pública:	Sí	- Rellenar Tabla 2. Experiencia mínima de 10 años en Administración Pública
Dedicación: 5 días a la semana de presencia en oficinas APB Palma	Sí, obligatoria	
Participación mínima de 1 proyectos de implantación del ENS y adaptación a la normativa de protección de datos	Sí	- Rellenar Tabla 3. Participación de proyectos de implantación del ENS y adaptación a la normativa de protección de datos
Certificación oficial el ámbito de la seguridad de la información	Sí	- Rellenar Tabla 4. Certificaciones oficiales en el ámbito de la seguridad de la información

Tabla 1. Titulaciones académicas:

Código	Título académico	Nivel MECES	Duración	Centro	F-expedición
T1					dd/mm/aaaa
...					
Tn					

Duración: duración oficial.



Tabla 2. Experiencia mínima de 10 años en proyectos para Administración Pública:

Empresa	Perfil ejercido en el proyecto	F-inicio	F-fin	Meses	Administración Pública
E1		dd/mm/aaaa	dd/mm/aaaa		
...					
En		dd/mm/aaaa	dd/mm/aaaa		

Tabla 3. Participación de proyectos de implantación del ENS:

Empresa	Descripción tareas realizadas	F-inicio	F-fin	Meses	Empresa/Organismo adaptado a ENS
P1		dd/mm/aaaa	dd/mm/aaaa		
...					
Pn		dd/mm/aaaa	dd/mm/aaaa		

Tabla 4. Certificación oficial en el ámbito de la seguridad de la información:

Nº	Certificación	Entidad/Organismo	F-certificado
C1			
...			
Cn			

El objetivo de las anteriores tablas es acreditar de manera clara que se cumplen los requisitos mínimos para cada perfil.

### **Medios de acreditación de la adscripción de medios**

La presentación de este anexo, se acompañará de los correspondientes títulos académicos, contratos laborales, certificados o informes de empresa, todo ello a los efectos de demostrar la capacitación técnica y la experiencia previa del personal que se piense vincular a la futura ejecución del contrato.

A) Para acreditar la formación:

A1- Titulación:

La titulación del personal adscrito se deberá acreditar con copia de los documentos expedidos por las entidades certificadoras (títulos universitarios, certificados de formación reglada, etc.). Cada nivel MECES engloba a todos los niveles inferiores, por lo que se aceptará cumplido el requisito de titulación cuando se presente una titulación igual o superior a la requerida.

A2- Certificaciones y Formación:

Presentación de las correspondientes copias de las certificaciones y certificados de las formaciones





B) Para acreditar la experiencia profesional del personal técnico adscrito, la empresa deberá aportar prueba documental de contratos de la cual pueda deducirse la acreditación del personal técnico, debiendo presentar **todos los documentos** que se relacionan a continuación:

B1.- Declaración responsable que acredite la participación del personal técnico en la ejecución de los contratos o proyectos que se declaren.

B2.- Documentos que acreditan la vinculación contractual del personal técnico con la empresa que ejecutó el contrato, se debe presentar:

- Contratos laborales, o vida laboral, que demuestre la vinculación del técnico con la empresa que ejecutó el proyecto/contrato, en el periodo indicado.
- Si el técnico participó en el proyecto a través de una tercera empresa, además de lo anterior, se debe aportar documentación que evidencie la subcontratación o, en su defecto, declaración responsable del correspondiente licitador en el presente expediente.
- En defecto de prueba documental de los puntos anteriores, se debe aportar un informe o certificado de la empresa contratante acreditando la participación del técnico o en su defecto, la declaración del respectivo licitador que acredite la participación del técnico en la ejecución del contrato.

B3.- Documentos que acreditan la existencia del contrato aportado:

- Se debe aportar prueba documental del contrato público o privado referenciado verificando una copia de este, o resolución de adjudicación, o certificados o informes de ejecución validados por la empresa licitadora correspondiente que indiquen nombre del proyecto, cliente, presupuesto de adjudicación, fecha de inicio y duración del contrato.
- En el caso de contratos con la Autoridad Portuaria de Baleares, se verifica la existencia de este a partir de la referencia aportada.
- En el caso de que el/la técnico/a haya participado en un proyecto interno para la empresa con la que mantiene una vinculación laboral y no para un tercero, no se exigirá prueba documental de la existencia de contrato para el desarrollo del proyecto, pero sí de la vinculación laboral con dicha empresa para ese periodo.

C) Para acreditar la vinculación contractual actual del personal técnico con la empresa propuesta como adjudicataria, podrá aportarse:

- Prueba documental (contratos laborales, vida laboral) de vinculación del personal técnico con la empresa.
- En el caso de que algunos recursos no se encuentren contratados por la empresa en el momento de acreditar los medios a adscribir (previa a la adjudicación), podrá presentarse un acuerdo de partes entre el futuro trabajador y la empresa licitante, de precontrato de trabajo que permita explicitar de forma fehaciente las condiciones de contratación y la obligatoriedad por parte de la empresa de ejecutar dicho acuerdo en caso de ser adjudicatario.





## 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 estimados a partir del convenio laboral de referencia “XVIII Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública (BOE núm. 87, de 9 de abril de 2023)” son los siguientes (sin IVA):

Perfiles	Precio/hora
Jefe/a de proyecto	64,00 €
Consultor/a experto en ciberseguridad	56,46 €

A estos precios hay que añadirle los costes indirectos que están constituidos por el beneficio industrial y los gastos generales de estructura.

- Beneficio industrial (BI): Se determina un beneficio industrial del 6,00%, a tenor de las ratios sectoriales de las sociedades no financieras que publica anualmente el Banco de España y aplicable sobre los costes salariales de los perfiles solicitados en el presente pliego.
- Gastos Generales (GG): Se fija un porcentaje para gastos generales del 13,00%, obtenidas de las ratios sectoriales de las sociedades no financieras que publica anualmente el Banco de España y aplicable sobre los costes salariales de los perfiles solicitados en el presente pliego.

Así mismo, se incluye a continuación el desglose de los servicios incluidos en esta contratación.

Estas cuantías se verán afectadas por el coeficiente de baja ofertado por el licitador.

Justificación Presupuesto			
Partida	Horas/año	Precio/h	Total
<b>CAP. 1. GESTIÓN DEL PROYECTO</b>			
<b>1.1. Gestión del proyecto</b>			<b>17.280,00 €</b>
Jefe/a de proyecto	270	64,00 €	17.280,00 €
<b>CAP. 2. DESARROLLO DE LAS FUNCIONES DEL ADMINISTRADOR DE SEGURIDAD (AS)</b>			
<b>2.1. Desarrollo de las funciones del Administrador de Seguridad (AS)</b>			<b>103.095,96 €</b>
Consultor/a experto de ciberseguridad	1.826	56,46 €	103.095,96 €
<b>PRESUPUESTO</b>			<b>120.375,96 €</b>
BI (6%) + GG (13%)			22.871,43 €
<b>IMPORTE LICITACION (IVA excluido): PRESUPUESTO + BI Y GG (1 AÑO)</b>			<b>143.247,39 €</b>
IVA (21%)			30.081,95 €
<b>PRESUPUESTO BASE DE LICITACIÓN (1 AÑO)</b>			<b>173.329,34 €</b>

