Junta de Andalucía

Consejería de Presidencia, Sanidad y Emergencias
Escuela Andaluza de Salud Pública

PLIEGO DE PRESCRIPCIONES TÉCNICAS

para la contratación de servicios de consultoría especializada para la adecuación, implantación y acompañamiento a la certificación de la Escuela Andaluza de Salud Pública en el Esquema Nacional de Seguridad (ENS)

Expediente: 202600039

Escuela Andaluza de Salud Pública (EASP)

Granada, julio de 2026

ÍNDICE

1. INTRODUCCIÓN

La Escuela Andaluza de Salud Pública (en adelante, EASP) es una entidad del Sector Público Andaluz, adscrita a la Consejería competente en materia de salud de la Junta de Andalucía, cuya misión es la mejora de la salud de la ciudadanía mediante la formación, la consultoría, la investigación y la cooperación en el ámbito de la salud pública y la gestión sanitaria.

Para el desarrollo de su actividad, la EASP dispone de una infraestructura tecnológica propia, articulada en torno a su Centro de Proceso de Datos (CPD), sobre la que se sustentan los sistemas de información y servicios digitales que dan soporte a sus procesos de negocio, tanto de uso interno como de servicio a la ciudadanía y a otras administraciones. La información tratada incluye datos de carácter personal, en ocasiones de categoría especial dado el ámbito sanitario en el que opera la entidad, lo que exige un nivel de protección reforzado.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), resulta de aplicación a todo el sector público en los términos establecidos en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En consecuencia, la EASP debe adecuar sus sistemas de información a los principios básicos y requisitos mínimos establecidos en dicho real decreto, y acreditar su conformidad mediante la correspondiente certificación.

2. ANTECEDENTES

Durante el primer semestre de 2026, la EASP ha llevado a cabo una evaluación de adecuación al Real Decreto 311/2022, en la que se han analizado las 73 medidas de seguridad del Anexo II del ENS, determinando su grado de implementación y el nivel de madurez conforme al modelo CMMI.

Las principales conclusiones de dicha evaluación son las siguientes:

- El nivel de madurez global actual de la organización se sitúa en torno al 45,75 %, frente al 80 % de referencia necesario para alcanzar el nivel de madurez objetivo (L4).
- El nivel de madurez es relativamente homogéneo entre los tres marcos evaluados: Marco Organizativo (43 %), Marco Operacional (47 %) y Medidas de Protección (44 %).
- La organización dispone de una base técnica de seguridad razonablemente implantada (protección perimetral, detección de amenazas y determinadas medidas de protección de servicios).
- Persisten carencias relevantes en la formalización, gestión y gobierno de la seguridad: ausencia de procesos documentados y formalizados, falta de un modelo de gestión continuo y medible, y debilidades en áreas clave como la gestión de incidentes, la continuidad del servicio, el análisis de riesgos y la gestión de proveedores.

Este diagnóstico evidencia la necesidad de abordar un proceso estructurado de adecuación al ENS que culmine con la certificación de conformidad de los sistemas de información incluidos en el alcance, expedida por una entidad de certificación acreditada.

El informe completo de la evaluación de adecuación se pondrá a disposición de los licitadores en las condiciones de confidencialidad descritas en el apartado 4 del presente pliego.

3. OBJETO DEL CONTRATO

El presente contrato tiene por objeto la prestación de servicios especializados para la adecuación, implantación y acompañamiento en el proceso de certificación del sistema de gestión de la seguridad de la información de la EASP en el Esquema Nacional de Seguridad (ENS), conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, y normativa complementaria de aplicación.

El alcance del contrato incluye, de forma integral, el análisis, diseño e implementación de las medidas de seguridad organizativas, operativas y de protección necesarias para garantizar el cumplimiento del ENS, principalmente en el CPD y en aquellos sistemas de información relevantes para la organización, infraestructuras tecnológicas, servicios digitales y procesos de negocio de la EASP, teniendo en cuenta la criticidad de los servicios prestados y la naturaleza especialmente sensible de la información tratada en el ámbito sanitario.

Asimismo, el contrato comprende:

- La definición e implementación de un plan de adecuación alineado con los requisitos del presente pliego.
- La elaboración y actualización del marco normativo de seguridad (políticas, normas, procedimientos e instrucciones técnicas).
- La propuesta de implantación de controles y salvaguardas, incluyendo medidas técnicas, organizativas y procedimentales, desarrolladas en un Plan Director.
- La realización de un análisis de riesgos conforme a metodologías reconocidas (MAGERIT u otras equivalentes).
- El soporte en los procesos de auditoría, incluyendo la auditoría interna y el acompañamiento en las auditorías externas de certificación.
- La preparación de la declaración de aplicabilidad y de la documentación exigida por el ENS.
- El soporte para la obtención de la certificación ENS.
- La transferencia de conocimiento y la formación al personal de la entidad.

La empresa adjudicataria deberá prestar los servicios con arreglo a criterios de calidad, cumplimiento normativo, confidencialidad, integridad y disponibilidad de la información, garantizando en todo momento la continuidad de los servicios y la protección de los datos personales, especialmente aquellos de categoría especial conforme a la normativa de protección de datos.

3.1 Codificación CPV

El objeto del contrato se corresponde con los siguientes códigos del Vocabulario Común de Contratos Públicos (CPV):

- 79417000-0: Servicios de consultoría en seguridad.
- 72220000-8: Servicios de consultoría en sistemas y consultoría técnica.
- 72222300-0: Servicios de tecnología de la información.
- 72253000-3: Servicios de soporte de sistemas informáticos.

4. ALCANCE

De conformidad con el ENS, la certificación de conformidad no se refiere a la organización en su conjunto, sino a los sistemas de información y servicios concretos que se incluyan en su alcance. En este sentido, el alcance de los trabajos del presente contrato comprende:

- El CPD de la EASP y los sistemas de información alojados en él, cuya categoría de seguridad prevista, conforme a los criterios del Anexo I del Real Decreto 311/2022, es ALTA.
- Los servicios digitales y sistemas de información relevantes para la actividad de la EASP que, como resultado de las tareas de identificación y categorización descritas en el apartado 5, se determine que deben formar parte del alcance de la certificación.

La delimitación definitiva del alcance de certificación (sistemas, servicios y categoría de seguridad de cada uno de ellos) constituirá una de las primeras tareas del contrato y deberá ser aprobada formalmente por la EASP.

La EASP pondrá a disposición de los licitadores el informe de evaluación de adecuación al ENS mencionado en el apartado 2, documento de carácter confidencial que será remitido previa solicitud al correo mariac.junco.easp@juntadeandalucia.es, debiendo aportar en dicha solicitud la cláusula de confidencialidad (Anexo II del presente pliego) debidamente cumplimentada y firmada por representante con poder suficiente.

5. DESCRIPCIÓN DE LOS SERVICIOS

Los servicios objeto del contrato se estructuran en tres fases secuenciales, junto con un servicio transversal de coordinación y seguimiento. Para cada fase se describen los objetivos, las tareas y los resultados (hitos y entregables) esperados.

5.1 Servicio transversal: coordinación y seguimiento

Servicio orientado a la gestión integral del proyecto mediante metodologías y estándares reconocidos, con el fin de garantizar la eficiencia, la productividad, la innovación y el cumplimiento de los plazos, la calidad y los objetivos establecidos. Comprende la planificación detallada de los trabajos, la celebración de reuniones de seguimiento periódicas, la elaboración de informes de avance y la gestión de riesgos y desviaciones del proyecto, conforme a lo dispuesto en el apartado 6 del presente pliego.

5.2 Fase I: Diagnóstico, categorización y planificación

5.2.1 Objetivos

- Delimitar formalmente el alcance de la certificación, identificando los servicios prestados por la EASP y los sistemas de información que los soportan.
- Determinar la categoría de seguridad de cada sistema conforme al Anexo I del RD 311/2022.
- Conocer y valorar los riesgos a los que están expuestos los activos de información incluidos en el alcance.
- Disponer de un plan de adecuación priorizado que guíe el resto de las actuaciones.

5.2.2 Tareas

- Identificación de servicios y sistemas. Inventario de los servicios prestados por la EASP y de los sistemas de información que los soportan, con la determinación de cuáles quedan dentro del alcance del ENS y su valoración por dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).
- Categorización de los sistemas. Propuesta motivada de categoría de seguridad para cada sistema, conforme al Anexo I del RD 311/2022, para su aprobación formal por la EASP.
- Realización del análisis de riesgos. Identificación, evaluación y tratamiento de los riesgos de seguridad de la información conforme al ENS y a la normativa de protección de datos (RGPD y LOPDGDD). La metodología empleada será conforme al ENS y a metodologías reconocidas (MAGERIT u otras equivalentes), utilizando preferentemente la herramienta PILAR del CCN.
- Análisis de impacto en el negocio (BIA) y plan de continuidad. Evaluación del impacto de posibles interrupciones de los servicios críticos y desarrollo de un Plan de Continuidad de Negocio que garantice la recuperación y continuidad operativa ante incidentes.
- Elaboración del plan de adecuación. Definición del plan de adecuación al ENS, alineado con los resultados de la evaluación de adecuación previa y del análisis de riesgos, con priorización de actuaciones, estimación de esfuerzos y calendario.
- Declaración de aplicabilidad provisional. Identificación de las medidas de seguridad del Anexo II del ENS aplicables a cada sistema, incluyendo, en su caso, las medidas compensatorias justificadas conforme a la guía CCN-STIC 819.

5.2.3 Resultados (hitos y entregables)

- Inventario de servicios y sistemas, con propuesta de alcance de certificación.
- Informe de categorización de los sistemas.
- Informe de análisis de riesgos.
- Análisis de impacto en el negocio (BIA) y Plan de Continuidad de Negocio.
- Plan de adecuación al ENS aprobado por la EASP.
- Declaración de aplicabilidad provisional.

5.3 Fase II: Desarrollo del marco normativo e implantación de medidas

5.3.1 Objetivos

- Dotar a la EASP de un marco normativo de seguridad completo, formalizado y alineado con el ENS.
- Implantar las medidas de seguridad organizativas, operacionales y de protección identificadas en el plan de adecuación.
- Capacitar y concienciar al personal de la EASP en materia de seguridad de la información.

5.3.2 Tareas

- Desarrollo o actualización de la Política de Seguridad. Elaboración o revisión de la Política de Seguridad de la organización, alineada con el ENS y la normativa vigente, definiendo los principios y directrices en materia de seguridad de la información, así como la estructura organizativa de seguridad (comité de seguridad, roles y responsabilidades).
- Desarrollo de la normativa de seguridad. Elaboración de las normas, procedimientos e instrucciones técnicas necesarias para el cumplimiento del ENS, priorizando las áreas con mayores carencias identificadas en la evaluación de adecuación (gestión de incidentes, continuidad del servicio, gestión de la configuración, gestión de proveedores, entre otras).
- Plan Director de implantación de controles. Propuesta de implantación de los controles y salvaguardas necesarios, incluyendo medidas técnicas, organizativas y procedimentales, desarrolladas en un Plan Director priorizado.
- Soporte a la implantación, mantenimiento, revisión y mejora continua. Asistencia técnica para la implantación y evolución del sistema de gestión de la seguridad, asegurando su mantenimiento, revisión periódica y mejora continua, incluyendo la definición de métricas e indicadores de seguimiento.
- Formación del personal. Diseño e impartición de acciones formativas dirigidas al personal para mejorar la concienciación y capacitación en seguridad de la información y cumplimiento normativo.

5.3.3 Resultados (hitos y entregables)

- Política de Seguridad aprobada por el órgano competente de la EASP.
- Cuerpo normativo de seguridad: normas, procedimientos e instrucciones técnicas.
- Plan Director de implantación de controles y salvaguardas.
- Evidencias de implantación de las medidas de seguridad y cuadro de indicadores.
- Plan de formación y concienciación ejecutado, con las evidencias correspondientes.

5.4 Fase III: Auditoría y certificación

5.4.1 Objetivos

- Verificar el grado de adecuación de los sistemas incluidos en el alcance a los requisitos del ENS.
- Obtener la certificación de conformidad con el ENS expedida por una entidad de certificación acreditada por ENAC.

5.4.2 Tareas

- Declaración de aplicabilidad definitiva. Consolidación de la declaración de aplicabilidad, con la identificación definitiva de las medidas de seguridad y refuerzos aplicables y, en su caso, de las medidas compensatorias justificadas conforme a la guía CCN-STIC 819.
- Auditoría interna de cumplimiento. Realización de una auditoría interna, conforme a los requisitos del artículo 31 y el Anexo III del RD 311/2022, para verificar el grado de adecuación al ENS y detectar desviaciones, proponiendo las medidas correctoras oportunas.
- Plan de acción. Elaboración de un plan de acción detallado que recoja las medidas necesarias para subsanar las no conformidades detectadas en la auditoría interna, con soporte a su resolución.
- Acompañamiento al proceso de certificación. Soporte especializado durante todo el proceso de certificación, incluyendo la preparación, la revisión documental y el apoyo durante la auditoría externa de certificación realizada por la entidad de certificación acreditada. Los costes de la entidad de certificación no forman parte del objeto del presente contrato.
- Cierre del servicio. Finalización del servicio mediante la entrega de un informe final que incluya el informe de auditoría interna, el estado de resolución del plan de acción y las recomendaciones para el mantenimiento y la mejora continua del sistema de gestión tras la certificación.

5.4.3 Resultados (hitos y entregables)

- Declaración de aplicabilidad definitiva.
- Informe de auditoría interna, con las evidencias correspondientes.
- Plan de acción y seguimiento de su resolución.
- Superación de la auditoría externa de certificación y obtención de la certificación de conformidad con el ENS.
- Informe de cierre del servicio.

6. ORGANIZACIÓN DEL TRABAJO

Todos los trabajos a realizar dentro del alcance de este contrato se ejecutarán bajo la dirección técnica de la persona responsable del contrato por parte de la EASP y dentro del marco general del proyecto. Todas las actividades y entregables deberán ser supervisados y aprobados por dicha persona responsable.

En virtud de lo dispuesto en el artículo 62 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), se designa como responsable del contrato a la persona Responsable de Sistemas de Información de la EASP, a quien corresponderá supervisar su ejecución y adoptar las decisiones y dictar las instrucciones necesarias con el fin de asegurar la correcta realización de los trabajos pactados.

6.1 No división en lotes

La EASP requiere que la solución objeto del contrato sea integral: las fases de diagnóstico y planificación, desarrollo e implantación, y auditoría y certificación deben ejecutarse de manera integrada y coordinada. No es asumible una segmentación de dichas prestaciones en lotes diferenciados dada la estrecha interrelación entre las tareas, la especialización de los perfiles necesarios y los altos niveles de confidencialidad requeridos por la naturaleza de los trabajos. La realización independiente de las prestaciones dificultaría la correcta ejecución del contrato desde el punto de vista técnico y comprometería los plazos del proceso de certificación.

6.2 Equipo de trabajo

Para la realización de los trabajos descritos, la empresa adjudicataria deberá aportar un equipo de trabajo mínimo conformado por CINCO (5) profesionales, con los siguientes perfiles y requisitos:

6.2.1 Jefe/a de proyecto (1)

- Grado o Licenciatura en Ingeniería Informática o Telecomunicaciones.
- Máster Universitario en Ciberseguridad.
- Más de CINCO (5) años de experiencia en proyectos de similar naturaleza.
- Al menos DOS (2) de las siguientes certificaciones: CISA, CISM, Lead Auditor ISO 27001, PMP o ITIL.

6.2.2 Consultores/as senior normativos (3)

- Grado o Licenciatura en Ingeniería Informática o Telecomunicaciones.
- Máster Universitario en Ciberseguridad.
- Más de TRES (3) años de experiencia en proyectos de similar naturaleza.
- Al menos TRES (3) de las siguientes certificaciones: CISA, CISM, CISSP, Lead Auditor ISO 27001, Lead Auditor ISO 22301.

6.2.3 Auditor/a jefe (1)

- Grado o Licenciatura en Ingeniería Informática o Telecomunicaciones.
- Más de TRES (3) años de experiencia en auditoría de sistemas de información.
- Certificación Lead Auditor ISO 27001 o CISA.
- Independencia respecto del equipo que ejecute las tareas de implantación, a fin de garantizar la objetividad de la auditoría interna prevista en la Fase III.

Si, a juicio de la EASP, alguno de los recursos propuestos no ejecutara los servicios descritos conforme a las exigencias del presente pliego, deberá ser sustituido a la mayor brevedad por otro profesional de igual o superior perfil, sin que ello afecte a la planificación de los trabajos prevista ni al coste del proyecto.

6.3 Metodologías

La empresa adjudicataria deberá entregar toda la documentación técnica y de gestión del proyecto, así como cualquier documentación adicional que, a juicio de la EASP, sea necesaria para alcanzar los objetivos del contrato.

Para la gestión de riesgos se empleará la metodología MAGERIT u otra equivalente reconocida, utilizando preferentemente la herramienta PILAR del Centro Criptológico Nacional (CCN). Para el desarrollo de los trabajos se tomarán como referencia las guías de la serie CCN-STIC aplicables, en particular las relativas a la adecuación al ENS, así como las herramientas y soluciones del CCN-CERT que la EASP determine (entre otras, AMPARO para la gestión del cumplimiento, en su caso).

Todos los productos obtenidos en el marco de este proyecto se adaptarán a los estándares de codificación, identidad corporativa y nomenclatura definidos por la EASP.

6.4 Marco de seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información, conforme al Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo. En concreto, se deberá asegurar el acceso, la integridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, informaciones y servicios utilizados por medios electrónicos que sean objeto de la presente contratación.

Se aplicarán las medidas de seguridad indicadas en el Anexo II del ENS, en función de los tipos de activos presentes en cada sistema de información y de las dimensiones de seguridad relevantes, considerando que el sistema principal objeto de certificación (CPD) recae en la categoría de seguridad ALTA conforme a los criterios establecidos en el Anexo I del ENS.

Además, se atenderá a las mejores prácticas sobre seguridad recogidas en la serie de documentos CCN-STIC, disponibles en la web del CCN-CERT (https://www.ccn-cert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz, y al marco normativo de seguridad TIC de la Junta de Andalucía que resulte de aplicación.

6.5 Gestión del proyecto

Los objetivos de la gestión del proyecto son garantizar que este se realiza en tiempo y forma, con los recursos previstos y cumpliendo los compromisos de entrega y calidad, y proveer las garantías de que la EASP dispondrá de los mecanismos necesarios para continuar con el mantenimiento del sistema de gestión de la seguridad una vez finalizado el proyecto.

Sin perjuicio de su posible ajuste al arranque del proyecto, se establecen los siguientes órganos de gestión:

Órgano de gestión	Funciones
Dirección de Proyecto de la EASP (responsable del contrato)	Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos. Asegurar el seguimiento de la planificación. Aprobar los contenidos de los trabajos y comunicárselos a la Jefatura de Proyecto. Velar por el nivel de calidad de los trabajos. Coordinar las entrevistas entre el personal usuario y técnico involucrado. Aprobar los resultados y certificaciones parciales o totales.
Jefatura de Proyecto de la empresa adjudicataria	Interlocución con la EASP. Dirección, seguimiento y control del proyecto. Generación de la documentación de control. Revisión de los trabajos y la documentación realizada por el equipo. Garantizar la calidad de los productos finales. Estructurar el funcionamiento y las tareas del equipo de trabajo.
Comité de Seguimiento (Dirección de Proyecto de la EASP y Jefatura de Proyecto de la adjudicataria)	Concreción de detalle de los plazos de ejecución. Control de las desviaciones frente a la planificación. Seguimiento de acuerdos y métodos de trabajo. Determinación de la puesta en marcha de las distintas fases. Adaptaciones del plan de ejecución para el mejor cumplimiento de los objetivos.
Comité Técnico (personal técnico de la EASP y consultores/as de la adjudicataria)	Información sobre el avance de los trabajos. Participación en las reuniones de seguimiento de carácter técnico, con toma de decisiones técnicas relacionadas con el contenido de los entregables, en particular la aprobación de sus versiones finales.

La gestión se llevará a cabo mediante tareas divididas en tres momentos: actividades de la fase de gestión inicial (plan de proyecto y planificación detallada), actividades de la fase de gestión de ejecución (seguimiento, informes de avance y gestión de desviaciones) y actividades de los procesos de gestión de finalización (cierre, transferencia y lecciones aprendidas).

6.6 Equipamiento y medios

El personal de la empresa adjudicataria prestará los servicios con sus propios medios y equipos de trabajo. Cuando resulte necesario el acceso a sistemas de la EASP, este se realizará conforme a los procedimientos y medidas de seguridad que la EASP establezca, previa autorización de la persona responsable del contrato.

6.7 Plazos

El contrato tendrá una duración de DOCE (12) meses desde su formalización. El inicio de los trabajos deberá producirse dentro de los QUINCE (15) días laborables siguientes a la formalización del contrato.

La planificación detallada de las fases descritas en el apartado 5 se acordará en el plan de proyecto, si bien deberá garantizar que la auditoría interna y el acompañamiento a la auditoría externa de certificación se realizan dentro del plazo de vigencia del contrato.

7. SOLVENCIA TÉCNICA Y PROFESIONAL

La solvencia técnica y profesional se acreditará por los siguientes medios:

7.1 Relación de servicios similares

Una relación de los principales servicios o trabajos realizados de igual o similar naturaleza que los que constituyen el objeto del contrato en el curso de los últimos TRES (3) años, en la que se indique el importe, la fecha y el destinatario, público o privado, de los mismos. El importe anual que el empresario deberá acreditar como ejecutado durante el año de mayor ejecución del periodo citado, en servicios de igual o similar naturaleza, debe ser igual al 70 por ciento del valor estimado del contrato, sin IVA.

Se acreditará mediante certificados expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público; cuando el destinatario sea un sujeto privado, mediante un certificado expedido por este o, a falta de dicho certificado, mediante una declaración del empresario.

Se considerará que un trabajo o servicio es de igual o similar naturaleza al que constituye el objeto del contrato si los tres primeros dígitos de los códigos CPV correspondientes al trabajo acreditado coinciden con los tres primeros dígitos de alguno de los códigos CPV indicados en el presente pliego. Supletoriamente, se considerarán aquellos trabajos que, no habiendo coincidencia en los primeros dígitos del CPV, tengan como objeto principal la realización de servicios de consultoría sobre cualquiera de las temáticas especificadas en el presente pliego.

7.2 Títulos académicos y profesionales

Títulos académicos y profesionales del equipo de trabajo que va a ejecutar el contrato, así como de los consultores encargados directamente del mismo, siempre que no se evalúen como criterio de adjudicación.

7.3 Acreditaciones de calidad y seguridad

Los licitadores deberán acreditar estar en posesión de las siguientes acreditaciones, que deberán mantenerse vigentes durante todo el periodo de prestación del servicio. Todas ellas guardan relación directa con el objeto del contrato y resultan proporcionadas a su finalidad, en los términos que se justifican a continuación:

ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información. El objeto del contrato consiste precisamente en el diseño, implantación y preparación para la certificación de un sistema de gestión de la seguridad de la información en la EASP. La certificación ISO/IEC 27001 acredita que el licitador aplica en su propia organización un sistema de esta naturaleza, auditado por un tercero independiente, lo que garantiza el dominio práctico —y no meramente teórico— de los procesos de análisis de riesgos, gestión de controles y mejora continua que deberá implantar en la EASP. Asimismo, dado que el adjudicatario accederá a información sensible sobre las infraestructuras y vulnerabilidades de la entidad, esta certificación garantiza que dicha información será tratada bajo controles de seguridad verificados.

ISO 22301 – Sistema de Gestión de Continuidad del Negocio. Entre las prestaciones del contrato se incluyen expresamente el análisis de impacto en el negocio (BIA) y la elaboración del Plan de Continuidad de Negocio de la EASP, áreas identificadas además como carentes en la evaluación de adecuación realizada en 2026. La certificación ISO 22301 acredita experiencia contrastada en la materia conforme al estándar internacional de referencia, lo que resulta determinante para la calidad de unos entregables que deben proteger la continuidad de servicios que tratan información del ámbito sanitario.

ISO 9001 – Sistema de Gestión de la Calidad. El contrato exige la producción de un volumen significativo de documentación (políticas, normativa, procedimientos, informes de auditoría) sometida a revisión y aceptación formal por la EASP, así como el cumplimiento de una planificación cuyo hito final —la certificación ENS— debe alcanzarse dentro del plazo de vigencia. La certificación ISO 9001 garantiza que el licitador dispone de procesos formalizados de control de calidad, gestión documental y tratamiento de no conformidades, reduciendo el riesgo de entregables deficientes o de desviaciones de planificación.

Certificación de conformidad con el Esquema Nacional de Seguridad (ENS), categoría MEDIA como mínimo. Resulta coherente exigir que quien vaya a conducir a la EASP hasta la certificación ENS haya superado con éxito ese mismo proceso en su propia organización, lo que acredita conocimiento directo del RD 311/2022, de las guías CCN-STIC y de la dinámica de las auditorías de certificación. Adicionalmente, conforme al artículo 2 del RD 311/2022, los sistemas de los prestadores de servicios al sector público deben cumplir el ENS cuando traten información de las entidades públicas, como ocurrirá en este contrato, por lo que la exigencia no es solo un criterio de solvencia sino una garantía de cumplimiento normativo durante la ejecución. Se fija la categoría MEDIA como mínimo por proporcionalidad, sin perjuicio de que la categoría ALTA —la exigida al CPD de la EASP— se valore como criterio de adjudicación.

De conformidad con los artículos 93 y 94 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, se admitirán los certificados equivalentes expedidos por organismos establecidos en cualquier Estado miembro de la Unión Europea, así como otras pruebas de medidas equivalentes de garantía de la calidad, de gestión de la seguridad de la información o de gestión de la continuidad del negocio que presenten los licitadores, siempre que acrediten un nivel de garantía análogo al exigido. En el caso de la certificación de conformidad con el ENS, dicha acreditación se ajustará a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, y en sus normas de desarrollo, debiendo estar expedida por una entidad de certificación acreditada conforme a los requisitos exigidos por el Centro Criptológico Nacional.

7.4 Certificados de buena ejecución específicos

- Certificados de ejecución en procesos de certificación ENS de al menos DOS (2) organismos en categoría ALTA.
- Experiencia en ciberseguridad en los TRES (3) últimos años en DOS (2) proyectos de cumplimiento normativo de clientes del sector salud.

8. NIVEL DE SERVICIO

8.1 Lugar de ejecución de los trabajos

La empresa adjudicataria realizará los trabajos, con carácter general, desde sus propias instalaciones (modalidad remota), contemplándose desplazamientos a la sede de la EASP en Granada para aquellas tareas que, por su naturaleza, deban ser ejecutadas presencialmente: sesiones de arranque, entrevistas, talleres de trabajo, acciones formativas presenciales, auditoría interna y acompañamiento durante la auditoría externa de certificación. Los gastos de desplazamiento correrán por cuenta de la empresa adjudicataria.

8.2 Horario de prestación del servicio

El servicio se prestará, de forma general, en horario laboral de la EASP, de lunes a viernes. Las actuaciones que puedan afectar a la disponibilidad de los sistemas se planificarán de común acuerdo con la persona responsable del contrato, pudiendo requerirse su ejecución fuera del horario habitual.

8.3 Seguimiento y plazos de entrega

Se celebrarán reuniones de seguimiento con periodicidad mínima mensual, sin perjuicio de las reuniones extraordinarias que la EASP convoque. La empresa adjudicataria presentará informes de avance con la misma periodicidad.

Los entregables serán revisados por la EASP, que podrá requerir su subsanación. La empresa adjudicataria dispondrá de un plazo máximo de DIEZ (10) días laborables para subsanar las deficiencias comunicadas, sin coste adicional. La aceptación formal de cada entregable corresponderá a la persona responsable del contrato.

9. CRITERIOS DE VALORACIÓN

Las ofertas se valorarán sobre un total de 100 puntos, conforme a la siguiente distribución: criterios sujetos a juicio de valor (40 puntos) y criterios evaluables de forma automática mediante fórmulas (60 puntos).

9.1 Valoración técnica (criterios sujetos a juicio de valor): 40 puntos

La valoración de este apartado se efectuará sobre la base de la memoria descriptiva presentada por los licitadores, que deberá describir de forma concreta y específica para este contrato el proceso de implantación de las medidas, con una extensión máxima de 25 páginas (formato DIN A4, letra Arial u otra equivalente, cuerpo 11). No se valorarán los contenidos de carácter genérico que no se refieran específicamente al objeto del contrato ni a la situación de partida de la EASP. La puntuación se distribuirá conforme a los siguientes subcriterios:

Subcriterio 1. Plan de trabajo y metodología (hasta 12 puntos). Se valorará la coherencia y el nivel de detalle de la planificación propuesta: desglose de fases, tareas y entregables; cronograma con hitos e identificación de tareas críticas; dimensionamiento y dedicación del equipo de trabajo; mecanismos de seguimiento, control de calidad y gestión de riesgos y desviaciones del proyecto; y viabilidad del conjunto dentro del plazo de ejecución del contrato.

Subcriterio 2. Enfoque técnico de la adecuación al ENS (hasta 12 puntos). Se valorará la solidez del planteamiento técnico de las Fases I y II: método propuesto para la identificación y categorización de sistemas conforme al Anexo I del RD 311/2022; planteamiento del análisis de riesgos (MAGERIT/PILAR), del análisis de impacto en el negocio y del plan de continuidad; enfoque para el desarrollo del marco normativo y del Plan Director de controles; y, en particular, la adaptación de la propuesta a los hallazgos de la evaluación de adecuación de 2026 y a la categoría ALTA prevista para el CPD.

Subcriterio 3. Auditoría interna y acompañamiento a la certificación (hasta 8 puntos). Se valorará el planteamiento de la Fase III: metodología de la auditoría interna conforme al artículo 31 y al Anexo III del RD 311/2022 y garantías de independencia del equipo auditor; tratamiento del plan de acción y de la subsanación de no conformidades; y estrategia de preparación y soporte durante la auditoría externa de la entidad de certificación.

Subcriterio 4. Formación y transferencia de conocimiento (hasta 8 puntos). Se valorará el plan de formación y concienciación propuesto (contenidos, número y duración de sesiones, colectivos destinatarios y materiales) y el planteamiento de la transferencia de conocimiento orientada a que la EASP pueda mantener de forma autónoma el sistema de gestión de la seguridad tras la finalización del contrato.

Metodología de valoración. Cada subcriterio se valorará de forma individualizada mediante la aplicación de la siguiente escala cualitativa sobre su puntuación máxima, debiendo motivarse expresamente en el informe técnico la asignación efectuada en cada caso: excelente —tratamiento completo, específico y plenamente adecuado al objeto del contrato— (100 %); bueno —tratamiento adecuado, con aspectos mejorables de escasa relevancia— (75 %); suficiente —tratamiento correcto pero incompleto o parcialmente genérico— (50 %); insuficiente —tratamiento superficial, genérico o con deficiencias relevantes— (25 %); no tratado o inadecuado (0 %).

La puntuación final será la suma aritmética de las puntuaciones obtenidas en los cuatro subcriterios, con un máximo de 40 puntos. No se tendrán en consideración, y quedarán excluidas de la licitación, las ofertas que no alcancen un umbral mínimo de 20 puntos (50 %) en el conjunto de los criterios sujetos a juicio de valor. El

resultado de esta valoración se incorporará al informe técnico correspondiente y se hará público con anterioridad a la apertura del sobre o archivo electrónico relativo a la proposición económica y demás criterios evaluables de forma automática, conforme al artículo 157 LCSP.

9.2 Criterios evaluables de forma automática por aplicación de fórmulas: 60 puntos

9.2.1 Oferta económica: 30 puntos

Conforme a la fórmula establecida en el Pliego de Cláusulas Administrativas Particulares.

9.2.2 Nivel de certificación ENS superior al mínimo exigido: 10 puntos

Se valorará que el licitador disponga de certificación ENS de categoría ALTA en el ámbito de los servicios objeto del contrato. Puntuación: ENS categoría ALTA acreditada, 10 puntos.

9.2.3 Certificados de buena ejecución adicionales: hasta 2 puntos

Se valorarán de forma adicional los certificados de ejecución en organismos públicos en categoría ALTA, a razón de UN (1) punto por certificado adicional aportado.

9.2.4 Experiencia del equipo de trabajo: hasta 8 puntos

- Se valorará de forma adicional hasta DIEZ (10) años de experiencia del jefe o la jefa de proyecto: 2 puntos.
- Se valorará de forma adicional hasta CINCO (5) años de experiencia de cada consultor/a: 6 puntos (2 puntos por cada consultor/a).

9.2.5 Certificación adicional: hasta 5 puntos

Se valorará de forma adicional disponer de habilitación de director/a de seguridad expedida por el Ministerio del Interior.

9.2.6 Reducción del tiempo de ejecución del contrato: hasta 5 puntos

Se valorará la reducción de los meses de ejecución del contrato, a razón de UN (1) punto por mes de reducción, siempre que la planificación ofertada resulte viable a juicio de la EASP.

Criterio	Puntuación máxima
Valoración técnica (memoria descriptiva)	40
Oferta económica	30
Certificación ENS categoría ALTA del licitador	10

Certificados de buena ejecución adicionales	2
Experiencia del equipo de trabajo	8
Habilitación de director/a de seguridad (Ministerio del Interior)	5
Reducción del tiempo de ejecución	5
TOTAL	100

10. CONDICIONES GENERALES

10.1 Propiedad de los trabajos

Todos los trabajos realizados dentro del ámbito de este contrato serán propiedad exclusiva de la EASP, sin que el contratista pueda conservarlos, obtener copia de los mismos o facilitarlos a terceros sin la expresa autorización de la EASP.

10.2 Transferencia tecnológica y del conocimiento

Durante la ejecución de los trabajos, la empresa adjudicataria se compromete a facilitar en todo momento a las personas designadas por la EASP la información y documentación que estas soliciten para disponer de un pleno conocimiento técnico de los trabajos realizados, de las circunstancias en que se desarrollan, de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos. La empresa adjudicataria asegurará que toda la documentación relativa al proyecto se encuentra actualizada a la finalización de los trabajos, de forma que la EASP pueda mantener de forma autónoma el sistema de gestión de la seguridad tras la finalización del contrato.

10.3 Control de calidad

Los trabajos realizados deberán cumplir lo exigido en el presente pliego y los estándares de la EASP, atendiendo a los principios de eficiencia y calidad de realización, y requerirán la aceptación formal de la EASP. Corresponden a la EASP los poderes de verificación y control establecidos en la LCSP, a través de la persona designada como responsable del contrato, sin que en ningún caso estas facultades puedan implicar el ejercicio de potestades directivas u organizativas sobre el personal de la empresa adjudicataria.

10.4 Garantía

La empresa adjudicataria garantizará los trabajos realizados durante un periodo mínimo de SEIS (6) meses desde la finalización del contrato, comprometiéndose a subsanar sin coste adicional los defectos o deficiencias imputables a la ejecución de los trabajos que se pongan de manifiesto durante dicho periodo, incluyendo las no conformidades documentales detectadas por la entidad de certificación cuya causa sea atribuible a los entregables del contrato.

10.5 Confidencialidad y protección de datos

La empresa adjudicataria y todo su personal quedan obligados a guardar secreto profesional respecto de la información a la que tengan acceso con ocasión de la ejecución del contrato, obligación que subsistirá tras

la finalización del mismo. El tratamiento de datos personales que, en su caso, resulte necesario se regirá por lo dispuesto en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), formalizándose el correspondiente contrato de encargado del tratamiento conforme al artículo 28 del RGPD.

10.6 Seguridad de la información

De conformidad con el artículo 2 del Real Decreto 311/2022, la empresa adjudicataria deberá garantizar durante toda la vigencia del contrato el cumplimiento de los requisitos del ENS que le resulten exigibles como prestadora de servicios al sector público, manteniendo vigente la certificación de conformidad requerida en el apartado 7.3 del presente pliego. Asimismo, deberá comunicar a la EASP, sin dilación indebida, cualquier incidente de seguridad que pueda afectar a la información o a los servicios objeto del contrato.

Conocido y aceptado en su totalidad, en Granada, a fecha de la firma electrónica.

48921221Z BLANCA DEL ROCIO BOTELLO (R: A18049635)

Firmado digitalmente por 48921221Z BLANCA DEL ROCIO BOTELLO (R: A18049635)
DN: Description=Ref:AEAT/AEAT0436/PUESTO 1/97927/02102025105619, SERIALNUMBER=IDCES-48921221Z, G=BLANCA DEL ROCIO, SN=BOTELLO DIAZ, CN=48921221Z BLANCA DEL ROCIO BOTELLO (R: A18049635), OID.2.5.4.97=VATES-A18049635, O=ESCUELA ANDALUZA DE SALUD PUBLICA SA, C=ES
Razón: Estoy aprobando este documento
Ubicación:
Fecha: 2026.07.17 14:30:29+02'00'
Foxit PDF Reader Versión: 2025.2.0

Fdo.: Blanca del Rocío Botello Díaz

Directora Gerente de la Escuela Andaluza de Salud Pública

ANEXO I. DOCUMENTACIÓN A DISPOSICIÓN DE LOS LICITADORES

La EASP pondrá a disposición de los licitadores que lo soliciten la siguiente documentación de carácter confidencial:

- Informe de evaluación de adecuación al Real Decreto 311/2022 de la EASP (junio de 2026), que incluye la situación actual y los hallazgos por marcos (organizativo, operacional y medidas de protección), el plan de acción con tareas y dimensionamiento, y el análisis de madurez.
- Información descriptiva de los sistemas preexistentes, su arquitectura y sus niveles de criticidad, a los efectos de la preparación de las ofertas.

Esta documentación será remitida previa solicitud al correo mariac.junco.easp@juntadeandalucia.es, debiendo aportar en dicha solicitud la cláusula de confidencialidad (Anexo II) debidamente cumplimentada y firmada por representante con poder suficiente, acreditando igualmente el poder de representación.

ANEXO II. CLÁUSULA DE CONFIDENCIALIDAD

D./Dña. [nombre y apellidos], con DNI [número], en nombre y representación de la empresa [razón social], con NIF [número], en calidad de [cargo], a los efectos de la obtención de la documentación confidencial referida en el Anexo I del Pliego de Prescripciones Técnicas del expediente 202600039,

SE COMPROMETE:

- A utilizar la documentación e información facilitadas por la EASP única y exclusivamente para la preparación de la oferta correspondiente al citado expediente de contratación.
- A no divulgar, publicar, ceder ni poner a disposición de terceros, total o parcialmente, dicha documentación e información, por ningún medio, sin la autorización previa, expresa y por escrito de la EASP.
- A restringir el acceso a la documentación e información al personal estrictamente necesario para la preparación de la oferta, garantizando que dicho personal conoce y asume las obligaciones de confidencialidad aquí establecidas.
- A destruir o devolver a la EASP la documentación facilitada, incluidas todas sus copias, una vez concluido el procedimiento de licitación, salvo obligación legal de conservación.
- A mantener las obligaciones de confidencialidad de forma indefinida, subsistiendo tras la finalización del procedimiento de licitación.

Y para que conste, firma la presente cláusula de confidencialidad.

En [lugar], a [día] de [mes] de [año].

Fdo.: [nombre, cargo y sello de la empresa]