ANÁLISIS DE LA DOCUMENTACIÓN DE SOLVENCIA TÉCNICA

Nº EXPEDIENTE: CH000-25-001

ACUERDO MARCO DE CIBERSEGURIDAD

LOTE 2

ÍNDICE

1. OBJETO.

El objeto del presente informe es recoger el análisis de la documentación técnica presentada por las empresas propuestas como adjudicatarias del **Expediente Número CH000-25-001– ACUERDO MARCO DE CIBERSEGURIDAD** en el **LOTE 2,** con la finalidad de valorar la acreditación de la solvencia técnica y profesional conforme a los criterios establecidos en el apartado 6 del Cuadro Resumen del Pliego de Cláusulas Administrativas Particulares, así como la documentación acreditativa de los CRITERIOS TÉCNICOS Y ECONÓMICOS VALORADOS MEDIANTE APLICACIÓN DE FORMULAS MATEMÁTICAS.

2. EMPRESAS PROPUESTAS COMO ADJUDICATARIAS.

El órgano de contratación de VEIASA ha propuesto a las empresas siguientes como adjudicatarias del ACUERDO MARCO por cumplir con los requisitos exigidos y haber obtenido la mayor puntuación, por lo que se ha procedido a solicitarles la documentación pre adjudicación requerida en los pliegos.

LOTE 2

- **INETUM ESPAÑA S.A.**

3. CRITERIOS DE SOLVENCIA TÉCNICA EXIGIDOS A LAS EMPRESAS ADJUDICATARIAS.

La Solvencia Técnica y Profesional exigida a los licitadores quedó establecida en el apartado 6 del Cuadro Resumen del Pliego de Cláusulas Administrativas, a través de los siguientes aspectos:

LOTE 2: ACREDITACIÓN DE PRESTACIÓN DE SERVICIOS

Los licitadores deberán acreditar haber prestado en los últimos tres años:

Al menos tres contratos de prestación de servicios de similares características que los que constituyen el objeto del presente contrato, esto incluye las tareas necesarias para la protección de la ciberseguridad a través de la prestación de servicios de prevención, protección, detección y respuesta.

La suma de los mismos, deberá ser al menos el 60% del importe de licitación de este lote.

Lote	Importe de licitación del Lote	Coeficiente	Valor mínimo de los contratos por lote
Lote 2	445.353,00 €	0,6	267.212,00 €

Los servicios y suministros realizados se acreditarán mediante certificados indicando su importe, fechas, destinatario y tipo de trabajos ejecutados, expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público o cuando el destinatario sea un comprador privado, mediante un certificado expedido por éste o, a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.

A efectos de determinar la correspondencia entre los trabajos ejecutados por el empresario y los que constituyen el objeto del contrato para este lote, se atenderá a la igualdad entre los todos los dígitos de alguno de los CPV del Lote 2.

- *32500000-8: Equipo y material para telecomunicaciones*
- *48732000-8: Paquetes de software de seguridad de datos*
- *72000000-5 Servicios TI: consultoría, desarrollo de software, Internet y apoyo*

LOTE 2. EQUIPO DE TRABAJO

Las empresas licitadoras deberán contar con un equipo de trabajo formado al menos por:

- *1 Gestor de Ciberseguridad que actuará también como Jefe de Proyecto.*
- *4 Especialistas en Ciberseguridad.*
- *4 Especialistas Técnicos.*

Cada miembro del equipo de trabajo deberá contar con al menos 3 años de experiencia en los últimos 5 años en servicios de características similares a los especificados en el PPT.

A estos efectos, los licitadores deberán presentar con la oferta, el ANEXO 11 del presente CR, junto a la vida laboral y currículum vitae, donde se describa la experiencia mínima exigida de los perfiles propuestos así como aquella que sea objeto de valoración conforme al apartado 8 del CR. Posteriormente, solo se acreditara la experiencia por el propuesto como adjudicatario, acompañando al Anexo 11, vida laboral y currículum ya aportados, certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.

LOTE 2. TITULACIÓN MÍNIMA PARA LOS DISTINTOS PERFILES

El personal adscrito a la prestación de servicios de vigilancia y monitorización de la ciberseguridad deberá contar con la siguiente titulación mínima:

- *Gestor de Ciberseguridad: Grado universitario en Ingeniería o (Nivel Meces 2, 3 o equivalente) en la especialidad de informática y/o telecomunicaciones.*
- *Especialista Técnico: Formación Profesional de Grado Medio o Técnico en FP, Bachiller superior, FP2 (Nivel MECES 1 o equivalente) en la especialidad de informática y/o telecomunicaciones.*
- *Especialista en Ciberseguridad: Formación Profesional de Grado Medio o Técnico en FP, Bachiller superior, FP2 (Nivel MECES 1 o equivalente en la especialidad de informática y/o telecomunicaciones.*

El requisito se acreditará mediante la aportación de copia de la titulación oficial correspondiente de cada miembro del equipo mínimo.

LOTE 2. CERTIFICACIONES DE FORMACIÓN ESPECIALIZADA

Las empresas licitadoras deberán acreditar, mediante copias de los correspondientes certificados exigidos, que el equipo mínimo de trabajo que presta los servicios de vigilancia y monitorización de la ciberseguridad, , dispone de alguna de las siguientes certificaciones, debiendo acreditarse que, cada uno de ellos, cuenta con al menos una certificación:

- *Seguridad de la información (CISSP, CISM)*
- *Auditoría de sistemas (CISA)*
- *LEAD AUDITOR en Sistemas de Gestión de la Continuidad del Negocio –ISO 22301- (expedido por organismo de certificación como AENOR, SGS, Bureau Veritas, BSI…) OSCP (Offensive Security Certified Professional)*
- *OSCE (Offensive Security Certified Expert)*
- *OSWE (Offensive Security Web Expert)*
- *CEH (Certified Ethical Hacker)*
- *CRISC (Certified in Risk and Information Systems Control)*
- *CISSP (CertifiedInformation Systems Security Professional)*
- *CPSA (Crest Practitioner Security Analyst)*
- *CRT (Crest Registered Tester)*
- *GREM (GIAC Reverse Engineering Malware)*
- *CompTIA Security+*

- *CSX (Cibersecurity Nexus) Cybersecurity Fundamentals Certificate*
- *Ethical Hacking+Phyton*
- *Tecnologías en materia de correlación de eventos y dispositivos de seguridad de la información.*

El requisito se acreditará mediante la aportación de copia de la titulación oficial correspondiente

LOTE 2. CERTIFICACIÓN ISO 27001 O EQUIVALENTE

Los licitadores dispondrán de un sistema de gestión de la seguridad de la información certificado conforme a la norma ISO/IEC 27001 o equivalente.

La acreditación de este criterio se realizará aportando el correspondiente certificado.

En el caso en que aporte una certificación equivalente, se deberá justificar dicha equivalencia mediante un documento (certificación) que permita verificar el cumplimiento de los requisitos. A efectos de demostrar la equivalencia de otra certificación aportada, deberá probarse que la certificación alternativa verifica las siguientes cuestiones en cada caso:

Requisitos que debe cumplir una certificación equivalente a la ISO/IEC 27001:

- *Verifica que la organización ha implementado y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI).*
- *Verifica que la organización dispone de políticas y procedimientos escritos que describen como manejar y proteger la información.*
- *Verifica que la organización lleva a cabo una identificación y evaluación de riesgos de seguridad de la información y establece medidas para mitigarlos.*
- *Verifica que la organización implementa medidas de seguridad para controlar el acceso a la información sensible y limitar el acceso solo a aquellos que tienen una necesidad legítima de conocerla.*
- *Verifica que la organización monitoriza su SGSI y lleva a cabo auditorías periódicas para verificar su eficacia.*
- *Verifica que la organización implementa un enfoque de mejora continua para su SGSI, es decir, que revisar y mejorar constantemente sus políticas, procedimientos y medidas de seguridad.*
- *Verifica que la organización capacita a su personal en materia de seguridad de la información, para asegurar que comprendan sus responsabilidades en la protección de la información.*

LOTE 2. CERTIFICACIÓN ISO 22301 SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Los licitadores deberán garantizar y acreditar que las instalaciones desde las que se prestan los servicios pueden mantener sus operaciones críticas frente a interrupciones mediante la aportación de la copia de la certificación ISO 22301(Sistema de Gestión de la Continuidad del Negocio), certificación equivalente. En el caso de no disponer de una certificación, se aportará declaración responsable de

persona con poder suficiente para ello y documentación acreditativa que lo justifique que permita verificar el cumplimiento de lo siguientes requisitos:

- *Disponer de un Análisis de Impacto en el Negocio (BIA) y una evaluación de riesgos actualizada.*
- *Disponer de Planes de Continuidad del Negocio (BCP) y de Recuperación ante Desastres (DRP) adaptados a cada área crítica de la organización.*
- *Realización de simulacros y pruebas periódicas para validar la eficacia de dichos planes.*
- *Disponer de Infraestructura y servicios clave con redundancia y respaldo (energía, conectividad, datos, sistemas).*
- *Disponer de personal capacitado para actuar de forma ágil y coordinada ante posibles incidentes.*
- *Realizar auditorías internas y revisiones externas regulares con consultores especializados, con el objetivo de fortalecer las capacidades de resiliencia y mantener los niveles de servicio.*
- *Medidas implantadas para mantener los niveles de servicio acordados con los clientes, minimizar los impactos y restablecer la operación normal en el menor tiempo posible, conforme a los objetivos de RTO (tiempo de recuperación) y RPO (pérdida aceptable de datos) definidos, en caso de contingencia.*

4. DOCUMENTACIÓN ACREDITATIVA DE LOS CRITERIOS TÉCNICOS Y ECONÓMICOS VALORADOS MEDIANTE APLICACIÓN DE FÓRMULA MATEMÁTICA.

En este apartado se enumera la documentación que deben presentar las empresas propuestas cómo adjudicatarias para justificar los criterios técnicos y económicos valorados mediante aplicación de fórmula matemática indicados en la declaración responsable del ANEXO 4-A.

CRITERIOS L2.C2. Certificación ISO/IEC 20000 Gestión de servicios de TI (máximo 4 puntos).

En caso de resultar adjudicatario, se deberá presentar copia de la certificación que haya declarado disponer.

CRITERIOS L2.C3 Experiencia del personal adscrito al equipo mínimo. (Máximo 21 puntos)

Se acreditara la experiencia por el propuesto como adjudicatario, acompañando al Anexo 11, vida laboral y currículum ya aportados, certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.

CRITERIOS L2.C7 Capacidades forenses (máximo 4 puntos).

En caso de resultar adjudicatario, se deberá presentar ficha técnica oficial del producto que haya declarado disponer.

CRITERIOS L2.C8 EDR Nativo (máximo 4 puntos).

En caso de resultar adjudicatario, se deberá presentar ficha técnica oficial del producto que haya declarado disponer.

CRITERIOS L2.C9 Sensores de Análisis de Tráfico de Red (máximo 4 puntos).

En caso de resultar adjudicatario, se deberá presentar ficha técnica oficial del producto que haya declarado disponer.

CRITERIOS L2.C10 Tecnologías de señuelo (máximo 4 puntos).

En caso de resultar adjudicatario, se deberá presentar ficha técnica oficial del producto que haya declarado disponer.

CRITERIOS L2.C11 Plataforma SIEM (máximo 5 puntos).

En caso de resultar adjudicatario, se deberá presentar certificado de ser Partner del fabricante y certificado de la ubicación del alojamiento en los términos exigidos.

5. ANÁLISIS DE SOLVENCIA TÉCNICA DE LOS LICITADORES PROPUESTOS COMO ADJUDICATARIOS DEL ACUERDO MARCO.

5.1. INETUM ESPAÑA S.A.

<u>Análisis del CRITERIO 1.- LOTE 2:</u> ACREDITACIÓN DE PRESTACIÓN DE SERVICIOS

El licitador presenta declaración responsable indicando de la prestación de TRES (3) servicios de similares características que los que constituyen el objeto del presente contrato, esto incluye las tareas necesarias para la protección de la ciberseguridad a través de la prestación de servicios de prevención, protección, detección y respuesta, realizados durante los últimos tres años, cuyas cuantías superan la cantidad de 267.212,00 €.

PROYECTO	CLIENTE	IMPORTE	AÑO DE EJECUCIÓN	Lote
Implantación Solucion EDR	Agencia Digital de Andalucia	4.024.545,10 € (*)	2024	Lote 2
Securización Correo Electrónico	AST-Gobierno de Aragón	2.852.923,88 €	2025	Lotes 2 y 3
Servicios RCJA. Servicios Troncales de Comunicaciones y Seguridad	Agencia Digital de Andalucia	651.839,34 € (**) 1.451.433,59 € (**)	2024 2025	Lotes 2 y 3

Para la acreditación del requisito presenta certificados expedidos por las entidades contratantes indicando su importe, fechas, destinatario, tipos de trabajos ejecutados y CPVs.

Los servicios ejecutados en lo últimos tres años computarían desde el plazo de presentación de las ofertas el 7/10/2025, por lo que el intervalo de tiempo en el que debe acreditar los contratos de los servicios, así como los importes requeridos sería desde el 7/10/2022 hasta el 7/10/2025.

En dichos certificados se puede comprobar:

- Que los servicios realizados son trabajos relacionados con servicios de prevención, protección, detección y respuesta en materia de ciberseguridad, entre otros trabajos.
- Que se han realizado en los últimos tres años.
- Que los importes de cada uno o la suma de los mismos superan el umbral requerido.
- Que los trabajos ejecutados en cada contrato contienen al menos uno de los CPVs del lote 2.

Por lo tanto, cumple el requisito de solvencia

Análisis del CRITERIO 2.- LOTE 2. EQUIPO DE TRABAJO

PERFIL	APORTA ANEXO 11	APORTA VIDA LABORAL	APORTA DOCUMENTACIÓN ACREDITATIVA DE LA EXPERIENCIA	CUMPLIMIENTO DE REQUISITO DE SOLVENCIA
Gestor de Ciberseguridad que actuará también como Jefe de Proyecto	**SI**	**SI**	**SI**	**SI**
Especialistas en Ciberseguridad 1	**SI**	**SI**	**SI**	**SI**
Especialistas en Ciberseguridad 2	**SI**	**SI**	**SI**	**SI**
Especialistas en Ciberseguridad 3	**SI**	**SI**	**SI**	**SI**
Especialistas en Ciberseguridad 4	**SI**	**SI**	**SI**	**SI**
Especialista Técnico 1	**SI**	**SI**	**SI**	**SI**
Especialista Técnico 2	**SI**	**SI**	**SI**	**SI**
Especialista Técnico 3	**SI**	**SI**	**SI**	**SI**
Especialista Técnico 4	**SI**	**SI**	**SI**	**SI**

Con fecha de 22/01/2026 se le requiere al licitador lo siguiente, otorgándole un plazo de 3 días hábiles:

En el punto 6 del CR se indica lo siguiente:

Las empresas licitadoras deberán contar con un equipo de trabajo formado al menos por:

- 1 Gestor de Ciberseguridad que actuará también como Jefe de Proyecto.

- 4 Especialistas en Ciberseguridad.

- 4 Especialistas Técnicos.

Cada miembro del equipo de trabajo deberá contar con al menos 3 años de experiencia en los últimos 5 años en servicios de características similares a los especificados en el PPT.

A estos efectos, los licitadores deberán presentar con la oferta, el ANEXO 11 del presente CR, junto a la vida laboral y currlículum vitae, donde se describa la experiencia mínima exigida de los perfiles propuestos así como aquella que sea objeto de valoración conforme al apartado 8 del CR. ***Posteriormente, solo se acreditara la experiencia por el propuesto como adjudicatario, acompañando al Anexo 11, vida laboral y currículum ya aportados, certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.***

Si bien se aporta por cada perfil propuesto en el ANEXO 11 el Currículum Vitae, Vida laboral, declaración responsable del empresario y declaración responsable de los técnicos, ***tendría que aportar para acreditar la experiencia por cada uno de dichos perfiles lo siguiente: Certificados expedidos o***

visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.

Por otro lado, del perfil especialista técnico 1, los datos indicados en el ANEXO 11 no coinciden con la vida laboral presentada. Tendría que aclarar la experiencia del perfil, ***que debe cumplir con la experiencia mínima requerida en las tareas indicadas.***

El licitador aporta en tiempo y forma la documentación, pero tras su revisión, es necesario volver a solicitar documentación acreditativa del criterio de solvencia.

Con fecha de 04/02/2026 se le requiere al licitador lo siguiente, otorgándole un plazo de 3 días hábiles:

Presenta la siguiente documentación para acreditar la experiencia de los perfiles:

- *CV*
- *Vida laboral en la que consta su experiencia en años.*
- *Declaración de INETUM de veracidad de datos y tenencia de documentación probatoria para aquellos proyectos adjudicados a INETUM*
- *Declaración de cada técnico, dando fe de la veracidad de su CV, particularmente de las empresas donde han trabajado anteriormente a INETUM. (No se considera documento acreditativo de la realización de la prestación)*

Al igual que en el expediente CF050-24-035 Servicios de Desarrollo y Mantenimiento al que INETUM hace mención en la respuesta a la aclaración, y aplicando el mismo criterio que en éste (así consta en el informe de análisis de la documentación de solvencia emitido en fecha 7/01/2026), se indica lo siguiente:

En base a la documentación acreditativa, declaración responsable, currículums y la vida laboral de cada uno de los perfiles, quedaría acreditada la experiencia que dichos perfiles han desarrollado en INETUM, no obstante, no se contabilizan a efectos de computar experiencia, los periodos en los que los perfiles han trabajado en otras empresas. Por este motivo, los siguientes perfiles no cumplen el requisito de solvencia:

- *Gestor de Ciberseguridad. La experiencia acreditada con la documentación aportada es de 2,76 años.*
- *Especialista Técnico 1. La experiencia acreditada con la documentación aportada es de 2,80 años.*
- *Especialista Técnico 3. La experiencia acreditada con la documentación aportada es de 1,63 años.*

Por lo tanto, ***tendría que aportar para acreditar la experiencia por cada uno de dichos perfiles lo siguiente: Certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.***

El licitador aporta en tiempo y forma lo siguiente:

- **Certificación CISA del Gestor de Ciberseguridad, indicando que:**

  La obtención de la certificación CISA requiere, conforme a los requisitos oficiales establecidos por ISACA, la acreditación previa de un mínimo de cinco (5) años de experiencia profesional verificable en funciones directamente relacionadas con auditoría de sistemas de información, control interno, gestión de riesgos tecnológicos y ciberseguridad, siendo dicha experiencia condición necesaria e indispensable para la concesión efectiva de la certificación, con independencia de la superación del examen teórico.

  Que, por tanto, la posesión de la certificación CISA, en los términos indicados, constituye un medio objetivo, verificable y reconocido internacionalmente de acreditación de experiencia profesional mínima superior a cinco (5) años, al haberse concedido únicamente tras la validación expresa de dicha experiencia por un organismo independiente y de reconocido prestigio internacional como ISACA. Motivo por el cual, dicha certificación debe entenderse como acreditativa de experiencias previas a Inetum en los ámbitos objeto del expediente de contratación por un plazo adicional de cinco (5) años.

Los 5 años que acredita mediante este certificado, obtenido antes del periodo trabajado en INETUM, sumado a los 2,76 años que había acreditado de experiencia en dicha empresa, suman 7,76 años de experiencia.

- **Declaración responsable del Especialista Técnico 1,** indicando que:

  Tal y como se exponía en el Anexo 11, previo a la experiencia laboral como trabajador por cuenta ajena de Inetum, dicho perfil desempeñaba sus labores como trabajador autónomo bajo el Régimen Especial de Trabajadores Autónomos "RETA", motivo por el cual y a efectos de aportación de documentación adicional, se acompaña declaración responsable identificando dicha condición además de los trabajos realizados y los destinatarios de los mismos en calidad de trabajador autónomo.

- **Del Especialista Técnico 3,** indica que:

  Inetum, no puede aportar certificaciones de trabajos que fueron ejecutados bajo la responsabilidad contractual de otras empresas, aun cuando las personas actualmente adscritas al contrato participasen materialmente en dichos servicios. Las certificaciones de experiencia en contratación pública y privada solo pueden ser emitidas por la entidad que dirigió, supervisó y asumió la responsabilidad técnica y jurídica de la ejecución, motivo por el cual resulta materialmente imposible aportar tal y como se solicita en el requerimiento "certificados expedidos o visados por el órgano competente" para aquellas experiencias del personal propuesto que fueron en empresas anteriores a Inetum.

  Que, no obstante, lo anterior, esta entidad mercantil ha presentado medios de acreditación válidos y alineados con lo así establecido en la normativa de aplicación, como son:

  - El Anexo 11, donde se detalla la experiencia concreta del personal propuesto y las funciones desarrolladas.

  - El CV firmado, que actúa como declaración responsable del profesional sobre su experiencia, con plena eficacia jurídica.

- La vida laboral, que constituye el documento oficial que acredita la realidad de las relaciones laborales y la vinculación temporal con los servicios descritos.

Entiende esta entidad mercantil, que, la combinación de estos documentos permite a la Administración verificar la experiencia alegada con total claridad, si bien y para completar la misma, esta entidad mercantil por medio del presente escrito aporta información adicional que acredita la experiencia identificada para los perfiles solicitados.

Con fecha de 12/02/2026 se le requiere al licitador lo siguiente, otorgándole un plazo de 3 días hábiles:

En base a la documentación acreditativa, declaración responsable, currículums y la vida laboral de cada uno de los perfiles, quedaría acreditada la experiencia que dichos perfiles han desarrollado en INETUM, no llegando a los tres años de experiencia exigidos.

- *Especialista Técnico 1. La experiencia acreditada con la documentación aportada es de 2,80 años.*
- *Especialista Técnico 3. La experiencia acreditada con la documentación aportada es de 1,63 años.*

Tras haber planteado la imposibilidad de aportar los certificados expedidos o visados por el órgano competente, para aquella experiencia del personal propuesto en empresas anteriores a Inetum, se les solicita que aporte ***los documentos obrantes en poder del mismo que acrediten la realización de la prestación o sustituyan a perfil correspondiente, con otro de iguales o superiores características al perfil incluido en su oferta y que fue objeto de valoración.***

Tras la solicitud de aclaraciones del día 12/02/2026, el licitador realiza un cambio de perfil para el Especialista Técnico 1 y Especialista Técnico 3, y aporta toda la documentación acreditativa de los requisitos de solvencia y valoración de los nuevos perfiles.

En base a la documentación acreditativa, declaración responsable, currículums y la vida laboral de cada uno de los perfiles, quedaría acreditada la experiencia que dichos perfiles han desarrollado en INETUM, siendo superior al mínimo exigido, **por lo que se cumple el requisito de solvencia.**

Análisis del CRITERIO 3.- LOTE 2. TITULACIÓN MÍNIMA PARA LOS DISTINTOS PERFILES

PERFIL	APORTA COPIA DE LA TITULACIÓN VÁLIDA	CUMPLE EL REQUISITO DE SOLVENCIA
Gestor de Ciberseguridad que actuará también como Jefe de Proyecto	**SI**	**SI**
Especialistas en Ciberseguridad 1	**SI**	**SI**
Especialistas en Ciberseguridad 2	**SI**	**SI**
Especialistas en Ciberseguridad 3	**SI**	**SI**
Especialistas en Ciberseguridad 4	**SI**	**SI**
Especialista Técnico 1	**SI**	**SI**
Especialista Técnico 2	**SI**	**SI**
Especialista Técnico 3	**SI**	**SI**
Especialista Técnico 4	**SI**	**SI**

Tras la solicitud de aclaraciones del día 12/02/2026, el licitador realiza un cambio de perfil para el Especialista Técnico 1 y Especialista Técnico 3, y aporta toda la documentación acreditativa de los requisitos de solvencia y valoración del nuevo perfil, comprobándose que las titulaciones aportadas son válidas.

Análisis del CRITERIO 4.- LOTE 2. CERTIFICACIONES DE FORMACIÓN ESPECIALIZADA

PERFIL	CERTIFICACIONES APORTADAS	APORTA ALGUNA DE LAS CERTIFICACIONES EXIGIDAS	CUMPLE EL REQUISITO DE SOLVENCIA
Gestor de Ciberseguridad que actuará también como Jefe de Proyecto	**CISM, CISA, AUDITOR LIDER 22301**	**SI**	**SI**
Especialistas en Ciberseguridad 1	**CISA**	**SI**	**SI**
Especialistas en Ciberseguridad 2	**CEH**	**SI**	**SI**
Especialistas en Ciberseguridad 3	**ZSCALER DIGITAL EXPERIENCE (ZDX)** **FORTINET CERTIFIED ASSOCIATE IN CYBERSECURITY**	Para cumplir con el criterio se solicitan certificaciones especializadas en "Tecnologías en materia de correlación de eventos y dispositivos de seguridad". El licitador aporta las certificaciones siguientes: Zscaler Digital Experience (ZDX) Administrator: ZDX es una solución de monitoreo basada en la	**SI**

		nube que mide la experiencia del usuario final, analizando el rendimiento desde el dispositivo, la red y la aplicación (SaaS, privada o en la nube). Permite a los equipos de TI identificar rápidamente si las interrupciones se deben al Wi-Fi, ISP o la aplicación, reduciendo el tiempo de resolución. La certificación acredita la competencia como administrador de la misma para medir el rendimiento y diagnosticar problemas de conectividad desde el dispositivo del usuario hacia las aplicaciones en la nube para reducir el tiempo de resolución de incidencias de red. **Por tanto, se considera que cumple el criterio de solvencia.** Fortinet Certified Associate in Cybersecurity: Esta certificación valida la capacidad para realizar operaciones técnicas en cortafuegos de próxima generación. **Por tanto, se considera que cumple el criterio de solvencia.**	
Especialistas en Ciberseguridad 4	**CROWDSTRIKE CERTIFIED FALCON ADMINISTRATOR**	Para cumplir con el criterio se solicitan certificaciones especializadas en "Tecnologías en materia de correlación de eventos y dispositivos de seguridad". El licitador aporta la certificación siguiente: Crowdstrike Certified Falcon Administrator: Esta certificación acredita conocimientos en EDR/XDR, gestión de endpoints y detecciones e incluye análisis de eventos de seguridad. **Por tanto, se considera que cumple el criterio de solvencia.**	**SI**
Especialista Técnico 1	**CROWDSTRIKE CERTIFIED FALCON ADMINISTRATOR** **SCS SYMANTEC DATA LOSS PREVENTION 15 ADMINISTRATOR** **SCS SYMANTEC CLOUD SOC-VERSIÓN 1 ADMINISTRATOR**	Para cumplir con el criterio se solicitan certificaciones especializadas en "Tecnologías en materia de correlación de eventos y dispositivos de seguridad". El licitador aporta las certificaciones siguientes: Crowdstrike Certified Falcon Administrator: Esta certificación acredita conocimientos en EDR/XDR, gestión de endpoints y detecciones e incluye análisis de eventos de seguridad. **Por tanto, se considera que cumple el criterio de solvencia.** SCS Symantec Data Loss Prevention 15 Administrator: Acredita la administración de una plataforma DLP, incluyendo monitorización y análisis de incidentes de seguridad. **Por tanto, se considera que cumple el criterio de solvencia.** SCS Symantec Cloud SOC – Administrator: Certifica competencias en detección, correlación y gestión de eventos de seguridad en entornos cloud. **Por tanto, se considera que cumple el criterio de solvencia.**	**SI**
Especialista Técnico 2	**APEX ONE AS A SERVICE CERTIFIED PROFESSIONAL** **DEEP SECURITY 20 CERTIFIED PROFESSIONAL**	Para cumplir con el criterio se solicitan certificaciones especializadas en "Tecnologías en materia de correlación de eventos y dispositivos de seguridad". El licitador aporta las certificaciones siguientes: Apex One as a Service Certified Professional: Esta certificación acredita conocimientos en EDR,	**SI**

		gestión de endpoints, gestión de eventos y detecciones de ciberseguridad. **Por tanto se considera que cumple el criterio de solvencia** Deep Security 20 Certified Professional: Esta certificación acredita conocimientos en seguridad de servidores (IPS, firewall, anti-malware) y gestión de eventos de ciberseguridad. **Por tanto se considera que cumple el criterio de solvencia**	
Especialista Técnico 3	**CLOUDFLAREACCREDITED SERVICES ARCHITECT** **FORCEPOINT GLOBAL TRAINING** **ACCREDITED CONFIGURATION ENGINEER (ACE)**	Para cumplir el criterio relativo a "Tecnologías en materia de correlación de eventos y dispositivos de seguridad de la información", el licitador aporta varias certificaciones: La certificación Cloudflare Accredited Services Architect acredita conocimientos en tecnologías de seguridad perimetral y de red, incluyendo protección DDoS, Web Application Firewall (WAF), Zero Trust, seguridad DNS, monitorización de tráfico y eventos de seguridad y arquitecturas de seguridad en entornos cloud. Estas competencias se encuentran directamente relacionadas con la vigilancia, monitorización y análisis de eventos de seguridad, así como con la operación de plataformas de ciberseguridad. **Se considera que cumple el criterio de solvencia**. Forcepoint es una plataforma de seguridad especializada en firewalls de nueva generación (NGFW), Data Loss Prevention (DLP), Web Security, CASB y monitorización y análisis de eventos de seguridad. La formación o certificación oficial acreditada por el fabricante certifica competencias en la configuración, operación y gestión de dispositivos y soluciones de seguridad, así como en la interpretación de los eventos generados por dichas tecnologías. **Se considera que cumple el criterio de solvencia.** La certificación Accredited Configuration Engineer (ACE), o certificación técnica equivalente de fabricante, acredita conocimientos en la configuración, operación y mantenimiento de dispositivos de seguridad tales como firewalls de nueva generación, sistemas de prevención de intrusiones (IPS), Web Application Firewalls y monitorización de eventos de seguridad. Estas competencias se alinean con el criterio exigido, al tratarse de tecnologías utilizadas para la vigilancia y monitorización de la ciberseguridad. **Se considera que cumple el criterio de solvencia.**	**SI**
Especialista Técnico 4	**MCAFEE: DATA LOSS PREVENT 10.0 DEV-LED DELTA KT (TECHNICAL)** **MCAFEE: NETWORK DATA LOSS PREVENTION 11.1 DELTA** **MCAFEE: ENTERPRISE SECURITY MANAGER**	Para cumplir con el criterio se solicitan certificaciones especializadas en "Tecnologías en materia de correlación de eventos y dispositivos de seguridad". El licitador aporta las certificaciones siguientes: McAfee: Data Loss Prevent 10.0 Dev-led Delta KT (Technical): acredita conocimienos sobre deteccion y correlacion de eventos relacionados con la exfiltración de datos haciendo uso de productos de seguridad de Mcafee	**SI**

	(SIEM) DEMO ON-DEMAND TRAINING	McAfee: Network Data Loss Prevention 11.1 Delta: similar a la anterior pero enfocada en tráfico de red. McAfee: Enterprise Security Manager (SIEM) Demo On-Demand Training: Su propósito principal es la agregación de logs de múltiples dispositivos de seguridad y la correlación de eventos para detectar amenazas complejas. Se considera que cada una de ella sirve para demostrar el cumplimiento del criterio de solvencia, especialmente si se tienen en cuenta de forma conjunta	

Con fecha 22/01/2026 se le solicita al licitador la siguiente aclaración:

En el punto 6 del CR se indica lo siguiente:

Las empresas licitadoras deberán acreditar, mediante copias de los correspondientes certificados exigidos, que el equipo mínimo de trabajo que presta los servicios de vigilancia y monitorización de la ciberseguridad, en conjunto, dispone de las siguientes certificaciones, debiendo acreditarse que, cada uno de ellos, cuenta con al menos una certificación:

- *Seguridad de la información (CISSP, CISM)*
- *Auditoría de sistemas (CISA)*
- *LEAD AUDITOR en Sistemas de Gestión de la Continuidad del Negocio –ISO 22301- (expedido por organismo de certificación como AENOR, SGS, Bureau Veritas, BSI…) OSCP (Offensive Security Certified Professional)*
- *OSCE (Offensive Security Certified Expert)*
- *OSWE (Offensive Security Web Expert)*
- *CEH (Certified Ethical Hacker)*
- *CRISC (Certified in Risk and Information Systems Control)*
- *CISSP (CertifiedInformation Systems Security Professional)*
- *CPSA (Crest Practitioner Security Analyst)*
- *CRT (Crest Registered Tester)*
- *GREM (GIAC Reverse Engineering Malware)*
- *CompTIA Security+*
- *CSX (Cibersecurity Nexus) Cybersecurity Fundamentals Certificate*
- *Ethical Hacking+Phyton*
- *Tecnologías en materia de correlación de eventos y dispositivos de seguridad de la información.*

El requisito se acreditará mediante la aportación de copia de la titulación oficial correspondiente.

Debe acreditar aportando las correspondientes certificaciones, que cada uno de los perfiles cuenta con al menos una certificación.

Tras la solicitud de aclaraciones del día 12/02/2026, el licitador realiza un cambio de perfil para el Especialista Técnico 1 y Especialista Técnico 3, y aporta toda la documentación acreditativa de los requisitos de solvencia y valoración del nuevo perfil, certificaciones aportadas son válidas.

El licitador aporta en tiempo y forma los certificados que se indican en la tabla, **por lo que cumple el requisito de solvencia.**

Análisis del CRITERIO 5.- LOTE 2. CERTIFICACIÓN ISO 27001 O EQUIVALENTE

Con fecha 22/01/2026 se le solicita al licitador la siguiente aclaración:

> *En el punto 6 del CR se indica lo siguiente:*
>
> *Los licitadores dispondrán de un sistema de gestión de la seguridad de la información certificado conforme a la norma ISO/IEC 27001 o equivalente. La acreditación de este criterio se realizará aportando copia del correspondiente certificado.*
>
> ***Debe aportar la certificación indicada o alguna equivalente que cumpla los requisitos indicados en el punto 6 del CR.***

El licitador aporta en tiempo y forma el Certificado del Sistema de Gestión de Seguridad de la Información en vigor, **por lo que cumple el requisito de solvencia.**

Análisis del CRITERIO 6.- LOTE 2. CERTIFICACIÓN ISO 22301 SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Con fecha 22/01/2026 se le solicita al licitador la siguiente aclaración:

> *En el punto 6 del CR se indica lo siguiente:*
>
> *Los licitadores deberán garantizar y acreditar que las instalaciones desde las que se prestan los servicios pueden mantener sus operaciones críticas frente a interrupciones mediante la aportación de la copia de la certificación ISO 22301(Sistema de Gestión de la Continuidad del Negocio), o certificación equivalente. La acreditación de este criterio se realizará aportando copia del correspondiente certificado.*
>
> *En el caso de no disponer de una certificación, se aportará declaración responsable de persona con poder suficiente para ello y documentación acreditativa que lo justifique que permita verificar el cumplimiento de lo siguientes requisitos:*
>
> - *Disponer de un Análisis de Impacto en el Negocio (BIA) y una evaluación de riesgos actualizada.*
> - *Disponer de Planes de Continuidad del Negocio (BCP) y de Recuperación ante Desastres (DRP) adaptados a cada área crítica de la organización.*
> - *Realización de simulacros y pruebas periódicas para validar la eficacia de dichos planes.*
> - *Disponer de Infraestructura y servicios clave con redundancia y respaldo (energía, conectividad, datos, sistemas).*
> - *Disponer de personal capacitado para actuar de forma ágil y coordinada ante posibles incidentes.*

- *Realizar auditorías internas y revisiones externas regulares con consultores especializados, con el objetivo de fortalecer las capacidades de resiliencia y mantener los niveles de servicio.*
- *Medidas implantadas para mantener los niveles de servicio acordados con los clientes, minimizar los impactos y restablecer la operación normal en el menor tiempo posible, conforme a los objetivos de RTO (tiempo de recuperación) y RPO (pérdida aceptable de datos) definidos, en caso de contingencia.*

Debe aportar la certificación indicada, equivalente o la Declaración Responsable que se indica en el punto 6 del CR.

El licitador aporta en tiempo y forma el Certificado del Sistema de Gestión de Seguridad de la Continuidad del Negocio, **por lo que cumple el requisito de solvencia.**

6. ANÁLISIS DE LA DOCUMENTACIÓN ACREDITATIVA DE LOS CRITERIOS TÉCNICOS Y ECONÓMICOS VALORADOS MEDIANTE APLICACIÓN DE FÓRMULA MATEMÁTICA.

6.1. INETUM ESPAÑA S.A.

CRITERIOS L2.C2. Certificación ISO/IEC 20000 Gestión de servicios de TI

Declara el cumplimiento de los requisitos establecidos por la norma ISO/IEC 20000 "Gestión de servicios de TI".	PRESENTA LA CERTIFICACIÓN DECLARADA	CUMPLE EL REQUISITO DE SOLVENCIA
SI	SI	SI

CRITERIOS L2.C3 Experiencia del personal adscrito al equipo mínimo.

PERFILES	Compromiso de experiencia por encima del mínimo exigido (3 años)	PRESENTA DOCUMENTACIÓN ACREDITATIVA QUE JUSTIFIQUE LA EXPERIENCIA DECLARADA	CUMPLE EL REQUISITO DE SOLVENCIA
Gestor de Ciberseguridad	>5 años	SI	SI
Especialista en Ciberseguridad	>5 años	SI	SI
Técnico en Ciberseguridad	>3 años	SI	SI

Con fecha de 22/01/2026 se le requiere al licitador lo siguiente, otorgándole un plazo de 3 días hábiles:

Si bien se aporta por cada perfil propuesto en el ANEXO 11 el Currículum Vitae, Vida laboral, declaración responsable del empresario y declaración responsable de los técnicos, ***tendría que aportar para acreditar la experiencia por cada uno de dichos perfiles lo siguiente: Certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.***

Además, en el ***CRITERIO DE VALORACIÓN L2.C3 Experiencia del personal adscrito*** *del punto 8 del CR, a una persona de cada perfil se le valoró la experiencia que se declaraba en el ANEXO 11 y por lo tanto,* ***en la documentación que debe aportar, debe justificar además de los 3 años exigidos para cumplir la solvencia, la experiencia indicada en el siguiente cuadro:***

PERFILES	Compromiso de experiencia por encima del mínimo exigido (3 años)
Gestor de Ciberseguridad	>5 años
Especialista en Ciberseguridad	>5 años

Técnico en Ciberseguridad	>3 años

El licitador aporta en tiempo y forma la documentación, pero tras su revisión, es necesario volver a solicitar documentación acreditativa del criterio de valoración.

Con fecha de 04/02/2026 se le requiere al licitador lo siguiente, otorgándole un plazo de 3 días hábiles:

Presenta la siguiente documentación para acreditar la experiencia de los perfiles:

- *CV*
- *Vida laboral en la que consta su experiencia en años.*
- *Declaración de INETUM de veracidad de datos y tenencia de documentación probatoria para aquellos proyectos adjudicados a INETUM*
- *Declaración de cada técnico, dando fe de la veracidad de su CV, particularmente de las empresas donde han trabajado anteriormente a INETUM. (No se considera documento acreditativo de la realización de la prestación)*

Al igual que en el expediente CF050-24-035 Servicios de Desarrollo y Mantenimiento al que INETUM hace mención en la respuesta a la aclaración, y aplicando el mismo criterio que en éste (así consta en el informe de análisis de la documentación de solvencia emitido en fecha 7/01/2026), se indica lo siguiente:

En base a la documentación acreditativa, declaración responsable, currículums y la vida laboral de cada uno de los perfiles, quedaría acreditada la experiencia que dichos perfiles han desarrollado en INETUM, no obstante, no se contabilizan a efectos de computar experiencia, los periodos en los que los perfiles han trabajado en otras empresas.

(…)

Por lo tanto, ***tendría que aportar para acreditar la experiencia por cada uno de dichos perfiles lo siguiente: Certificados expedidos o visados por el órgano competente cuando el destinatario sea una entidad de sector público, y cuando el destinatario sea un sujeto privado, mediante un certificado expedido por esta o a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación.***

Además, en el ***CRITERIO DE VALORACIÓN L2.C3 Experiencia del personal adscrito*** *del punto 8 del CR, a una persona de cada perfil se le valoró la experiencia que se declaraba en el ANEXO 11 y por lo tanto,* ***en la documentación que debe aportar, debe justificar además de los 3 años exigidos para cumplir la solvencia, la experiencia indicada en el siguiente cuadro.***

PERFILES	**Compromiso de experiencia por encima del mínimo exigido (3 años)**	
Gestor de Ciberseguridad	>5 años	El perfil propuesto NO acredita lo indicado en el anexo 4-A. (Ni el mínimo exigido de 3 años)
Especialista en Ciberseguridad	>5 años	El perfil propuesto NO acredita lo indicado en el anexo 4-A. El perfil que más experiencia acredita es el Especialista en Ciberseguridad 1, con 2,9 años de experiencia por encima del mínimo exigido.

A título ejemplificativo le indicamos que, para acreditar la experiencia, se podrá aportar documentación necesaria para obtener certificaciones de ciberseguridad que requieran un mínimo de experiencia como requisito, siempre y cuando en la documentación se incluya firma o sello de la empresa que acredita la experiencia.

El licitador aporta en tiempo y forma la siguiente documentación:

- **Certificación CISA del Gestor de Ciberseguridad**, que acredita 5 años de experiencia tal y cómo se indicó en el apartado Análisis del CRITERIO 2.- LOTE 2. EQUIPO DE TRABAJO, que sumados a los 2,76 años que acredita de experiencia en dicha empresa suman 7,76 años de experiencia.

- Declaración Responsable en la que indica lo siguiente entre otros asuntos:

  Inetum, no puede aportar certificaciones de trabajos que fueron ejecutados bajo la responsabilidad contractual de otras empresas, aun cuando las personas actualmente adscritas al contrato participasen materialmente en dichos servicios. Las certificaciones de experiencia en contratación pública y privada solo pueden ser emitidas por la entidad que dirigió, supervisó y asumió la responsabilidad técnica y jurídica de la ejecución, motivo por el cual resulta materialmente imposible aportar tal y como se solicita en el requerimiento "certificados expedidos o visados por el órgano competente" para aquellas experiencias del personal propuesto que fueron en empresas anteriores a Inetum.

  Que, no obstante, lo anterior, esta entidad mercantil ha presentado medios de acreditación válidos y alineados con lo así establecido en la normativa de aplicación, como son:

  - El Anexo XI, donde se detalla la experiencia concreta del personal propuesto y las funciones desarrolladas.

  - El CV firmado, que actúa como declaración responsable del profesional sobre su experiencia, con plena eficacia jurídica.

  - La vida laboral, que constituye el documento oficial que acredita la realidad de las relaciones laborales y la vinculación temporal con los servicios descritos.

Por lo tanto, teniendo en cuenta los 6,95 años de experiencia que se indican en el Anexo 11 de trabajos realizados en otras empresas del sector, coincidentes con los periodos indicados en Vida Laboral aportada acreditarían el compromiso de experiencia de >5 años por encima del mínimo exigido de (3 años), indicado en el Anexo 4-A.

- **Certificación CISA del Especialista en Ciberseguridad.**

Los 5 años que acredita mediante este certificado, obtenido antes del periodo trabajado en INETUM, sumado a los 5,9 años que había acreditado de experiencia en dicha empresa, suman 10,9 años de experiencia, es decir, 7,9 años por encima del mínimo exigido (3 años), cumpliendo por tanto el compromiso de >5 años indicado en el Anexo 4-A.

CRITERIOS L2.C7 Capacidades forenses

Declara que ofrece como parte de su solución herramientas integradas para recopilación de evidencias que faciliten la realización de análisis forenses.	PRESENTA FICHA TÉCNICA OFICIAL DEL PRODUCTO	CUMPLE EL REQUISITO DE SOLVENCIA
SI	SI	SI

CRITERIOS L2.C8 EDR Nativo

Declara que ofrece como parte de su solución, al menos una herramienta con capacidades EDR nativa.	PRESENTA FICHA TÉCNICA OFICIAL DEL PRODUCTO	CUMPLE EL REQUISITO DE SOLVENCIA
SI	SI	SI

CRITERIOS L2.C9 Sensores de Análisis de Tráfico de Red

Declara que ofrece como parte de su solución, al menos una herramienta con capacidades para recopilar eventos basados en IDS y monitorizar las peticiones DHCP y DNS.	PRESENTA FICHA TÉCNICA OFICIAL DEL PRODUCTO	CUMPLE EL REQUISITO DE SOLVENCIA
SI	SI	SI

CRITERIOS L2.C10 Tecnologías de señuelo

Declaración de disponer de los siguientes SEÑUELOS	PRESENTA FICHA TÉCNICA OFICIAL DEL PRODUCTO	CUMPLE EL REQUISITO DE SOLVENCIA
Honeypot	SI	SI
Honey Users	SI	SI
Honey Files	SI	SI
Honey Credentials	SI	SI

CRITERIOS L2.C11 Plataforma SIEM

OFRECE como parte de su solución una herramienta SIEM con las siguientes características	PRESENTA FICHA TÉCNICA OFICIAL DEL PRODUCTO	CUMPLE EL REQUISITO DE SOLVENCIA
Servicio llave en mano basado en una tecnología en la que el licitador tenga el máximo nivel de Partner con el fabricante	SI	SI
Datacenter que sea una infraestructura propia del adjudicatario, situado en territorio nacional para evitar posibles latencias a la hora de prestar los servicios y certificado al menos en TIER III	SI	SI

Con fecha 22/01/2026 se le solicita al licitador la siguiente aclaración:

> *En el CRITERIO DE VALORACIÓN L2.C11 Plataforma SIEM, se le valoró lo siguiente, indicado en el Anexo 4-A:*
>
> *OFRECE como parte de su solución una herramienta SIEM con las siguientes características*
>
> *Datacenter que sea una infraestructura propia del adjudicatario, situado en territorio nacional para evitar posibles latencias a la hora de prestar los servicios y certificado al menos en TIER III*
>
> ***El documento que se adjunta para justificar el cumplimiento del criterio es una certificación ENS, no una certificación TIER III. Se debe aportar certificación en TIER III o superior del centro de datos que soporta la infraestructura del SOC.***

El licitador aporta en tiempo y forma el Certificado oficial de TIER IV, cuyo nivel de disponibilidad, redundancia y resiliencia es superior al mínimo exigido en el pliego, correspondiente al datacenter, que soporta la Infraestructura SOC propuesta, **por lo que cumple el requisito de solvencia.**

7. PROPUESTA.

Tras el estudio de la documentación aportada por la empresa**.** se concluye que la empresa **INETUM ESPAÑA S.A.,** ACREDITA la solvencia técnica y profesional requerida en el LOTE 2 de esta licitación.

Sevilla a fecha de la firma

27302346N JOSE LUIS NAVAS (C:A41398645)

Firmado digitalmente por 27302346N JOSE LUIS NAVAS (C:A41398645)
Fecha: 2026.02.18 10:33:50 +01'00'

Jose Luis Navas Mora
Responsable de Seguridad de la Información