Comunidad de Madrid

Dirección General de Salud Digital
CONSEJERÍA DE DIGITALIZACIÓN

Exp.: A/SER-047045/2023

INFORME DE LA PUNTUACIÓN OBTENIDA POR LOS LICITADORES EN LOS CRITERIOS DEPENDIENTES DE JUICIO DE VALOR (TÉCNICOS), PARA LA ADJUDICACIÓN CORRESPONDIENTE A LA LICITACIÓN DEL CONTRATO DE SERVICIOS DE "OFICINAS DE SEGURIDAD Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN DEL SERVICIO MADRILEÑO DE SALUD – 2 LOTES" A ADJUDICAR POR PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS.

A la licitación del contrato se han presentado las siguientes empresas:

Lote 1: CIPHERBIT, S.L.U.; IZERTIS, S.A.; MNEMO EVOLUTION & INTEGRATION SERVICES S.A.; S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.; TECNOLOGÍAS PLEXUS, S.L.; UTE ACCENTURE CREMADES

Lote 2: ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.; AYESA ADVANCED TECHNOLOGIES, S.A.; DEVOTEAM DRAGO, S.A.; EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.; FUJITSU TECHNOLOGY SOLUTIONS S.A.; INETUM ESPAÑA, S.A.; LAMBDA SEC S.L.; PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.; PROCESIA PROYECTOS Y SERVICIOS, S.L.; MNEMO EVOLUTION & INTEGRATION SERVICES S.A.; S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.; TECNOLOGÍAS PLEXUS, S.L.; TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.

Al revisar la documentación administrativa en la mesa celebrada el 4 de abril de 2024, la mesa de contratación acuerda rechazar la proposición presentada por la empresa DEVOTEAM DRAGO S.A.

En la mesa para la apertura de los criterios de juicio de valor celebrada el día 22 de abril de 2023 se abrió el sobre Nº 2 con la información que las empresas han presentado, para la evaluación de los criterios de valoración técnicos, según juicio de valor.

La mesa de contratación acuerda excluir a la empresa UTE ACCENTURE CREMADES por no haber subsanado toda la documentación que le había sido requerida.

Según el Pliego de Cláusulas Administrativas los criterios cuya cuantificación dependen de un juicio de valor (Técnico), son los siguientes:

LOTE 1

9.1. Criterios cuya cuantificación depende de un juicio de valor para el Lote 1 (hasta 36 puntos)

9.1.1. Propuesta y enfoque metodológico para la gestión de la OSSI (hasta 16 puntos)

Las empresas licitadoras incluirán dentro de su catálogo de productos entregables, una estrategia de modelo de gobierno definiendo las herramientas y mecanismos necesarios para llevar a cabo el seguimiento, monitorización y control de las diferentes dimensiones que conforman el gobierno del Servicio de Seguridad y Privacidad. Además, en la propuesta deberá figurar el detalle de toda la documentación que será generada como consecuencia del gobierno del servicio.

Se incluirá documentación detallada de la metodología y el enfoque y adaptación de dicha metodología a las particularidades del SERMAS y la DGSD. Se valorará la metodología global, las diferentes fases y para cada una de las líneas de trabajo y servicios, así como el plan general de aseguramiento de la calidad y de continuidad del servicio.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de adecuación de la propuesta y del enfoque metodológico para la gestión de la OSSI, con un detalle amplio de las actividades, herramientas y mecanismos necesarios para el seguimiento, monitorización y control y de toda la documentación generada.

- BUENO (75%): Buen nivel de adecuación de la propuesta y del enfoque metodológico para la gestión de la OSSI, con buen nivel de detalle de las actividades, herramientas y mecanismos necesarios para el seguimiento, monitorización y control y de toda la documentación generada.

- SUFICIENTE (50%): Nivel suficiente de adecuación de la propuesta y del enfoque metodológico para la gestión de la OSSI, con suficiente nivel de detalle de las actividades, herramientas y mecanismos necesarios para el seguimiento, monitorización y control y de toda la documentación generada.

- ESCASO (0%): Escaso nivel de adecuación de la propuesta y del enfoque metodológico para la gestión de la OSSI, con insuficiente nivel de detalle de las actividades, herramientas y mecanismos necesarios para el seguimiento, monitorización y control y de toda la documentación generada.

9.1.1. Propuesta y enfoque metodológico para la gestión de la OSSI (máx. 16 puntos)	
EMPRESA	PUNTUACIÓN
CIPHERBIT, S.L.U.	16
IZERTIS, S.A.	12
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0
TECNOLOGÍAS PLEXUS, S.L.	12

CIPHERBIT, S.L.U.:

Detalla extensamente la aproximación metodológica de su solución, incluyendo todos los aspectos referidos a la gobernanza, documentación, herramientas y diferentes planes, aporta un buen conocimiento de la organización sanitaria adaptándose a los problemas del SERMAS, tanto en seguridad como en protección de datos. Desarrolla modelo de gobierno aportando matriz de roles y responsabilidades, propone utilización herramientas diversas incluidas las propias CCN. Proporciona soporte sobre diversas herramientas. Ofrece apoyo adicional en aspectos concretos. La valoración es excelente.

IZERTIS, S.A.

Hace un planteamiento amplio, pero no desarrolla los aspectos relacionados con la protección de datos (derechos ARCO, solicitudes de terceros, etc.); tampoco desarrolla los aspectos relacionados con los servicios sanitarios. Propone metodologías diversas como DevSecOps, Itil y Metrica 3. Utiliza herramientas CCN-CERT (PILAR, ANA, etc.). La valoración es buena.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Realiza una propuesta muy general sin concretar detalles sobre la organización sanitaria, detalla la planificación del servicio documentación y actividades, pero no propone herramientas como apoyo metodológico. El enfoque del servicio hace más hincapié en la calidad (propone un comité de calidad, seguridad y medioambiental y un gestor de calidad), que a la seguridad y protección de datos ya que ofrece apoyo al CISO del SERMAS y la dedicación del responsable coordinador nos es exclusiva. La valoración es escaso.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.

No desarrolla aspectos relacionados con la organización sanitara y los problemas de protección de datos, el planteamiento de la organización del servicio es muy genérico. Citan normativa ya derogada del ENS. Tampoco abunda en propuestas de herramientas como apoyo a su metodología. La valoración es escaso.

TECNOLOGÍAS PLEXUS, S.L.

Proporciona un detalle amplio del servicio, apoyado sobre la herramienta GRC Risk4All. Con una aproximación a la protección de datos y la seguridad centrados en Sanidad.

Pero, no especifica control de costes, presenta una organización basada en comités (director,

seguimiento del servicio y tantos comités operativos como funciones a desarrollar) lo que resulta muy complejo de gestionar, tampoco aborda la previsión de futuras necesidades. La valoración es buena.

9.1.2. Otro servicio de interés (hasta 5 puntos)

Los licitadores podrán incluir en su oferta otro servicio en el ámbito de seguridad de los datos. La oferta de este servicio implica la obtención de hasta 5 puntos, siempre que se considere de interés para el SERMAS y esté correctamente justificada la necesidad y el detalle del servicio.

Regla de puntuación:

- EXCELENTE (100%): Inclusión en la oferta de un servicio de un máximo nivel de interés para el SERMAS que ofrezca una gran necesidad y justificación del mismo, con un máximo nivel de detalle del servicio.

- BUENO (75%): Inclusión en la oferta de un servicio de un buen nivel de interés para el SERMAS que ofrezca una necesidad y justificación del mismo, con un buen nivel de detalle del servicio.

- SUFICIENTE (50%): Inclusión en la oferta de un servicio de un adecuado interés para el SERMAS que ofrezca un nivel suficiente de necesidad y justificación del mismo, con un adecuado nivel de detalle del servicio.

- ESCASO (0%): Inclusión en la oferta de un servicio de escaso interés para el SERMAS que ofrezca un escaso nivel de necesidad y justificación del mismo, con insuficiente detalle del servicio.

9.1.2. Otro servicio de interés (máx. 5 puntos)	
EMPRESA	PUNTUACIÓN
CIPHERBIT, S.L.U.	5
IZERTIS, S.A.	2,5
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0
TECNOLOGÍAS PLEXUS, S.L.	2,5

CIPHERBIT, S.L.U.:

Proponen una serie de servicios de valor añadido, que se consideran muy convenientes:

Evaluación del impacto e introducción de nuevas tecnologías y transformación digital en el ámbito sanitario.

Plan de actuación DPD a medida.

Servicio de técnicas avanzadas de anonimización y seudonimización y cuantificación del riesgo de reidentificación de los datos personales.

Servicios de Vigilancia Digital y soporte en casos suplantación de identidad online. Ejercicio Red Team anual.

Herramienta de administración del estado de seguridad (HADES). Soporte en la operación de herramientas GRC (no la aportan).

Asesoramiento en selección, despliegue y configuración de Herramientas y Recursos CCN-CERT y soluciones avanzadas de Mercado.

Desarrollar una versión avanzada del asistente ROSSI 2.0 basado en IA.

La valoración es excelente

IZERTIS, S.A.

Proponen para la gestión auditorías y superficie de exposición, utilizar la herramienta del Centro Criptológico Nacional ANA (Automatización y Normalización de Auditorías) como soporte a las auditorías.
Ofrecen un equipo de expertos en recuperación de incidentes que aborden la respuesta a incidentes. Si bien este equipo es ofertado por el resto de licitadores en el apartado de los servicios variables, por lo que no constituye un servicio adicional. No contempla acciones en materia de protección de datos. La valoración es suficiente.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Propone la implantación de una herramienta de gestión de ciberseguridad desarrollada por la propia empresa para proyectos de I+D+i (otras propuestas lo incluyen fuera de este apartado, en la propia propuesta metodológica). También propone un servicio de inteligencia para simulaciones, no se adapta al entorno sanitario y hace referencia a entornos financieros. No hace referencia a protección de datos. La valoración es escaso.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.

Propone tres servicios de potencial interés adicional (consultoría Forensic Readiness, Alerta Temprana, Modelado de Amenazas) con un nivel de descripción teórico y alcance general poco adaptado al entorno sanitario y sus particularidades. El servicio de alerta temprana lo proporcionan CCN-CERT y la Agencia Madrid Digital, por lo que no es valorable como adecuado. No contempla acciones en materia de protección de datos. La valoración es escaso.

TECNOLOGÍAS PLEXUS, S.L.

Propone dos servicios adicionales. La gestión de riesgos de terceros, aplicable a otros proveedores/agentes involucrados con DGSD/SERMAS, automatizado mediante la herramienta Risk4ll. En el ámbito de la protección de datos personales, proponen un sistema de gestión y la implementación de un sistema de privacidad de la información basado en la ISO/IEC 27701, basándose en la misma herramienta. La valoración es suficiente.

9.1.3. Plan de Formación y Comunicación (hasta 6 puntos)

Plan de Formación y Comunicación, indicando el contenido propuesto para el material formativo, metodología y duración de las sesiones formativas, métodos de evaluación del cumplimiento de objetivos, la calidad, el valor técnico del plan, la adecuación al ámbito sanitario, así como el detalle de las actividades a realizar, la precisión de los objetivos, la metodología a seguir adaptándose a las necesidades, los entregables, etc.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de adecuación del Plan de Formación y Comunicación con el máximo nivel de detalle en todos los puntos requeridos en el criterio.

- BUENO (75%): Buen nivel de adecuación del Plan de Formación y Comunicación con buen nivel de detalle en todos los puntos requeridos en el criterio.

- SUFICIENTE (50%): Suficiente nivel de adecuación del Plan de Formación y Comunicación con suficiente nivel de detalle en todos los puntos requeridos en el criterio.

- ESCASO (0%): Escaso nivel de adecuación del Plan de Formación y Comunicación con insuficiente nivel de detalle en todos los puntos requeridos en el criterio.

9.1.3. Plan de Formación y Comunicación (máx. 6 puntos)	
EMPRESA	PUNTUACIÓN
CIPHERBIT, S.L.U.	6
IZERTIS, S.A.	3
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0
TECNOLOGÍAS PLEXUS, S.L.	3

CIPHERBIT, S.L.U.:

Aportan una definición a detallada de la realización del Plan anual de formación, incluyendo ejemplos en cada fase. Aportan una herramienta de formación moodle SMARTFENSE. Proponen indicadores para medir la efectividad de este plan. Los contenidos del plan cubren un amplio abanico de necesidades, incluyendo realización ciberejercicios dentro de este apartado. El plan de comunicación contempla la publicación de nuevos procedimientos, normativas, estrategia de ciberseguridad, etc... La valoración es excelente.

IZERTIS, S.A.

Propone un plan de formación coherente y detallado, incluyendo propuestas de indicadores para mejora continua. No formula aportaciones ni comentarios sobre plan de comunicación. La valoración es suficiente.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Propone un plan de formación general sobre las acciones a desarrollar, sin entrar de forma específica en detalles. Se basa en una metodología de mejora continua a alto nivel. No propone aspectos referidos al plan de comunicación, más allá de aquellas acciones referidas a la formación. Propone algunas webinars con algún contenido no aplicable al SERMAS (como pagos en línea). La valoración es escaso.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.

Propone un plan de formación escaso, basado en acciones muy limitadas, con poca flexibilidad en cuanto a los destinatarios de las mismas. No propone aspectos referidos al plan de comunicación. La valoracion es escaso.

TECNOLOGÍAS PLEXUS, S.L.

Propone los planes de una forma coherente, detallada y basado en la gestión sobre una herramienta de soporte para todo el servicio Risk4all. Incluye la realización de ciberejercicios. El plan de comunicación propone, entre otros medios, utilizar redes sociales (puede no ser adecuado para el conjunto del SERMAS) y portal web. La valoración es suficiente.

9.1.4. Plan de concienciación (hasta 4 puntos)

Idoneidad y coherencia del plan de concienciación, valorando su adaptación al ámbito sanitario, una planificación anual, formatos adaptados a las necesidades de la época o los usuarios destino, detalle de las propuestas y la medición de su eficacia.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de adecuación del plan de concienciación con el máximo nivel de detalle de las propuestas de las medidas para su realización.
- BUENO (75%): Buen nivel de adecuación del plan de concienciación con un buen nivel de detalle de las propuestas de las medidas para su realización.
- SUFICIENTE (50%): Suficiente nivel de adecuación del plan de concienciación con un nivel adecuado de detalle de las propuestas de las medidas para su realización.
- ESCASO (0%): Insuficiente nivel de adecuación del plan de concienciación con un escaso nivel de detalle de las propuestas de las medidas para su realización.

9.1.4. Plan de concienciación (máx. 4 puntos)	
EMPRESA	PUNTUACIÓN
CIPHERBIT, S.L.U.	4
IZERTIS, S.A.	2
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	3
TECNOLOGÍAS PLEXUS, S.L.	3

CIPHERBIT, S.L.U.:

Propone un plan muy detallado en base a las necesidades del SERMAS, donde su valor aumenta al incluir la plataforma SMARTDEFENSE, microvideos con CANVA y el enfoque centrado en las necesidades del ámbito sanitario. Tiene en cuenta los riesgos y amenazas del ámbito sanitario, la protección del dato y el cumplimiento de la normativa; y áreas más específicas de la salud. Además propone una serie amplia de ciberejercicios distintos. Propone utilizar cuadro de mando con indicadores y un informe final del Plan. La valoración es excelente.

IZERTIS, S.A.

Define aspectos muy generales referidos a la concienciación y un plan para el desarrollo de actividades referidas a la misma, incluyendo propuesta de indicadores para el seguimiento y no aparece concretado a las particularidades del entorno sanitario. La valoración es suficiente.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Únicamente desarrolla los ciberejercicios de forma teórica. No tiene en cuenta la concienciación en materia de protección de datos, por lo que falta concreción y adaptación al entorno sanitario. La valoración es escaso.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.

Aporta la metodología ProtectIT para trabajar la concienciación de los trabajadores, constituye un enfoque original del plan a desarrollar, y realiza una descripción amplia de las acciones a realizar. Diseña acciones orientadas a diferentes colectivos y se adapta a entornos sanitarios (simulación de incidente en una UCI). No aporta plataforma de elerning. La valoración es buena.

TECNOLOGÍAS PLEXUS, S.L.

Detalla las acciones a acometer dentro del ámbito de la concienciación (12 acciones en materia de seguridad y 12 en materia de protección de datos), incluyendo las áreas temáticas y documentación e indicando la disposición para su elaboración y adaptación de estas a nuevas necesidades, sin especificar acciones sobre colectivos concretos. En su propuesta vincula estrechamente al plan de formación y contempla desarrollar una serie de entregables que apunta, sin desarrollar. La valoración es buena.

9.1.5. Cumplimiento de normativa (hasta 5 puntos)

Detalle del plan de adecuación al ENS, donde se detalle el alcance inicial, con un plan de adecuación realista para ir certificando y aumentando ese alcance. Además, se valorará la propuesta para actualizar los análisis de riesgos de los diferentes sistemas de información.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de coherencia y calidad del plan de adecuación al ENS con el detalle del cronograma desde el alcance inicial y máximo nivel de detalle de las propuestas de actualización de los análisis de riesgos.
- BUENO (75%): Buen nivel de coherencia y calidad del plan de adecuación al ENS con el detalle del cronograma desde el alcance inicial y buen nivel de detalle de las propuestas de actualización de los análisis de riesgos.

- SUFICIENTE (50%): Suficiente nivel de coherencia y calidad del plan de adecuación al ENS con el detalle del cronograma desde el alcance inicial y adecuado nivel de detalle de las propuestas de actualización de los análisis de riesgos.

- ESCASO (0%): Insuficiente nivel de coherencia y calidad del plan de adecuación al ENS con el detalle del cronograma desde el alcance inicial y escaso nivel de detalle de las propuestas de actualización de los análisis de riesgos.

9.1.5. Cumplimiento de normativa (máx. 5 puntos)	
EMPRESA	PUNTUACIÓN
CIPHERBIT, S.L.U.	5
IZERTIS, S.A.	3,75
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	2,5
TECNOLOGÍAS PLEXUS, S.L.	2,5

CIPHERBIT, S.L.U.:

Detalla profusamente acciones para acometer el plan de adecuación al ENS de los sistemas de una forma gradual, incluyendo la utilización de herramientas y alineamiento con los estándares y normativas a aplicar, particularizándolos al ámbito de la salud y, concretamente, al ámbito de servicio del contrato. Tiene en cuenta el soporte tanto a la certificación del ENS como al Lote 2 para el proceso de auditoría interna. Propone un servicio en el que, además de la adecuación al ENS, tiene en cuenta otros servicios de materia legal, como son el asesoramiento técnico y apoyo en servicios de Administración electrónica, otras peticiones legal-TIC y la monitorización permanente del entorno legal. La valoración es excelente.

IZERTIS, S.A.

Describe de forma general acciones para acometer el plan de adecuación al ENS, incluyendo un calendario estimado de acciones. Contempla la normativa aplicable tanto ENS como RGPD, pero no detalla el alcance del proyecto ni adapta la oferta a la realidad del SERMAS. La valoración es buena.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Detalla de una forma general acciones para acometer el plan de adecuación al ENS, pero no incluye detalle de actividades ni planificación. No concreta el planteamiento para las particularidades de la asistencia sanitaria. La calificación es escaso

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.

Tiene un plan de adecuación muy ambicioso en los tiempos, sin detallar el alcance global. Desarrolla en detalle cada fase , incluyendo los entregables a realizar. En el desarrollo de las fases incluye el acompañamiento en la auditoria de certificación en ENS. No contempla análisis de la situación en materia de protección de datos. La calificación es suficiente.

TECNOLOGÍAS PLEXUS, S.L.

El plan de adecuación se basa en el perfil de cumplimiento específico muy centrado en el ENS, apoyándose en la herramienta GRC. Establece prioridades para abordar este cumplimiento, centrándose en historia clínica. Por lo demás, se centra en los análisis de riesgos y no detalla tanto el resto de fases para adecuarse al ENS, ni tampoco las cuestiones sobre protección de datos. La valoración es suficiente.

LOTE 2

9.2. Criterios cuya cuantificación depende de un juicio de valor para el Lote 2 (hasta 36 puntos)

9.2.1. Propuesta de alcance, metodología y tipología de las auditorías (hasta 36 puntos)

Se valorará con hasta 36 puntos el alcance, metodología y tipología de las auditorías, en base a los criterios indicados a continuación.

9.2.1.1. Visión global e integradora. Metodología, Descripción y Contenido de los Trabajos (hasta 20 puntos)

Se valorará un plan de proyecto común, que aúne los objetivos perseguidos tanto para el cumplimiento del ENS como del GDPR. Asimismo, se valorará globalmente la calidad, el valor técnico del proyecto y la concreción de la oferta, así como el detalle de las actividades a realizar, la precisión de los objetivos, la metodología a seguir, los entregables, etc.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de adecuación de la visión global e integradora, con un máximo nivel de detalle de la metodología, descripción y contenido de los trabajos.

- BUENO (75%): Buen nivel de adecuación de la visión global e integradora, con un buen nivel de detalle de la metodología, descripción y contenido de los trabajos.

- SUFICIENTE (50%): Suficiente nivel de adecuación de la visión global e integradora, con un adecuado nivel de detalle de la metodología, descripción y contenido de los trabajos.
- ESCASO (0%): Insuficiente nivel de adecuación de la visión global e integradora, con un escaso nivel de detalle de la metodología, descripción y contenido de los trabajos.

9.2.1.1. Visión global e integradora. Metodología, Descripción y Contenido de los Trabajos (máx. 20 puntos)	
EMPRESA	PUNTUACIÓN
ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.	10
AYESA ADVANCED TECHNOLOGIES, S.A.	10
EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.	15
FUJITSU TECHNOLOGY SOLUTIONS, S.A.	15
INETUM ESPAÑA, S.A.	10
LAMBDA SEC S.L.	0
MNEMO EVOLUTION & INTEGRATION SERVICES S.A	10
PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.	10
PROCESIA PROYECTOS Y SERVICIOS, S.L.	15
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0
TECNOLOGÍAS PLEXUS, S.L.	20
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.	10

ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.:

En la auditoria de protección de datos establece dos fases, describe actividades de cada fase de forma secuencial y no plantea seguimiento de medidas.
Respecto a las auditorias ENS se remite a la metodología MAGERIT y herramienta PILAR, Aporta valor en la implantación de las medidas de seguridad para la adecuación al ENS. Identifica amenazas y calcula riesgos, pero no incluye el perfil de cumplimiento especifico sanidad (PEC SALUD Guía CCN STIC 891). Propone diseñar una serie de planes de acción y establecer sinergias entre auditorias ENS y protección de datos. No aporta herramientas o metodología adicional. La valoración es suficiente.

AYESA ADVANCED TECHNOLOGIES, S.A.:

Contempla la coordinación con Lote 1 y otras entidades (Agencia Madrid Digital, etc.). Propone metodología ITIl y PMBOK (utilización de Lean y Agile). Respecto auditorias de protección de datos establece tres fases con el alcance previsto en PPT. Describe fases, actividades a revisar y grado de cumplimiento alcanzado, pero no concreta al ámbito del SERMAS pues habla de varios Delegados de Protección de Datos (DPD).
En seguridad, además de la auditoría, propone una serie de medidas de adaptación y seguimiento para su adecuación, sigue las recomendaciones del perfil de cumplimiento especifico de salud (PCE SALUD CCN) y de Cibersalud. Valora nivel de cumplimiento ENS según parámetros de categoría y nivel de sistema que describe.
Aporta valor gracias a un enfoque metodológico basado en la ISO 19011, con un amplio detalle de cada fase. Contempla planificación de las auditorías y plan de implantación describe entregables en cada fase de auditoría. No indica de forma expresa la utilización de herramientas CCN, aunque se remite a las guías. Aporta refuerzo con unidades internas especializadas de la empresa. La valoración es suficiente.

EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.:

Proporciona un amplio detalle del servicio, con fases claras (planificación, prestación y devolución) y metodología en cada una (incluye mitigación riesgos) y entregables de cada una de ellas. Para la prestación del servicio propone metodología ITIL, PMI y SCRUM, con utilización de las herramientas CCN y guías CCN-STIC (incluye PCE SALUD). Establece coordinación con oficina de seguridad y sinergias entre el desarrollo de auditorías de ENS y protección de datos, con seguimiento de las recomendaciones y mejoras. Como propuesta de valor añadido aporta la creación de formularios interactivos con Ms Forms, Bookings para agendar las reuniones, PowerBI para cuadro de mando integral donde realizar el control y seguimiento, así como una línea de soporte técnico a los centros para consultas.

Se quedan fuera del alcance los tratamientos de la DGSD y de la C. Sanidad, ya que se refiere en el alcance a los sistemas de información que dan servicio al tratamiento de datos del SERMAS en su ámbito de actuación, no menciona la Consejeria de Sanidad. La valoración es buena.

FUJITSU TECHNOLOGY SOLUTIONS, S.A.:

Proporciona un enfoque conjunto de auditoría de protección de datos y seguridad. Con un enfoque de cumplimiento a la NIS2 (normativa UE en ciberseguridad) y PEC SALUD. Como propuesta de valor añadido destacar: observatorio de normativa aplicable por posibles cambios y actualizaciones y un grupo de expertos adicionales a lo previsto en PPT.

Para la realización auditoria de protección de datos de carácter personal plantea fases claras y establece acciones, pero no propone entregables, si establece estos en la fase de realización de la auditoria y la posterior de seguimiento de recomendaciones. Como metodología se basa en la ISO19011, la ISO 27701 y 27002, recomendaciones para auditorías de tratamientos que incluyan IA (AEPD) y guías de auditorías del ISMS Forum.

En las auditorias del ENS distingue tres fases (implantación, extensión y finalización) establece tareas en cada fase y define entregables de forma detallada. Se apoya en metodología MAGERIT y herramienta PILAR del CCN. La valoración es bueno.

INETUM ESPAÑA, S.A.:

INETUM tiene un conocimiento claro del objetivo de las auditorías, así como de sus beneficios.
Aporta una definición detallada de la metodología, con los diferentes dominios a auditar.
Para el ENS, no tiene en cuenta el PCE SALUD.

No propone herramientas adicionales, las de CCN y las que pueda poner DGSD. Propone plan de adaptación al ENS usando metodología Magerit y herramienta Pilar. La valoración es suficiente.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

Para las relativas a protección de datos establece dos fases (no aporta metodología). Propone la utilización de de herramientas del CCN. No concreta propuestas en función situación SERMAS, ajustándose estrictamente al PPT en cuanto a centros a auditar. Respecto a las auditorias ENS no incluye el PEC SALUD, no se tiene en cuenta la especificidad de sanidad en el ámbito de la seguridad. Establece tres fases (planificación, extensión y finalización). La oferta no aporta un valor añadido por encima de lo previsto en PPT. Valoración suficiente.

LAMBDA SEC S.L.:

En la propuesta se hace referencia a la regulación de seguridad obsoleta, tanto el RD 3/2010, como versiones obsoletas de la ISO 27001 y 27002. Los objetivos no están detallados adecuadamente y son muy generales. No tiene en cuenta el Perfil de cumplimiento específico de salud. La valoración es escaso.

PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.:

Deja abierta la metodología a usar, hablando por un lado de estándares internacionales que podrán ser incluidos, y luego detalla una metodología basada en tres planos: operativo, táctico y estratégico. Pero sin detallar en qué fases o actividades se van a basar.

Respecto a las auditorias propone realizar un análisis previo a su inicio para concretar alcance y fases en ambos tipos de auditorías y utilizar, como metodología propia, un Marco de Control de Auditoria de Referencia.

En las auditorías de protección de datos se apoya en el RGPD estructura cuatro fases, que concretará en un análisis previo, tampoco concreta en la situación del SERMAS la descripción que realiza es generalista.

En las auditorias del ENS contempla seguir PCE SALUD (CCN) como marco de referencia y empleo herramientas CCN. Propone una metodología detallada para ENS correcta con cuatro fases, donde incluye una propuesta de procesos y sistemas de información a auditar, incluyendo análisis de riesgos y plan de implantación. Como punto de valor incluye en la oferta su observatorio de tendencias regulatorias y sesiones formativas para el personal de la DGSD. La valoración es suficiente.

[redacted]

PROCESIA PROYECTOS Y SERVICIOS, S.L.:

En su ámbito de acción plantea una metodología de gestión de auditorías común para ambos tipos: protección de datos y ENS. Presenta las fases de gestión del ciclo de vida de las auditorias, de forma correcta, y culmina con un seguimiento de acciones correctivas y preventivas, se basan en ISO 19011. No mencionan al SUMMA112 y se centran en hospitales, primaria y servicio centrales. Incluye referencias normativas ajustándose al PEC SALUD.
En las auditorias sobre protección de datos realiza un planteamiento admisible y muy convencional. En materia de ENS propone seguir metodología MAGERIT y herramienta PILAR del CCN, partiendo de un análisis de situación actual.
Proponen un plan de implantación global y, como valor añadido, un cuadro de mando de seguimiento mensual con una serie de informaciones. Aportan tres indicadores adicionales de Acuerdos de Nivel de Servicio, para su seguimiento. La valoración es bueno.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.:

Propone una metodología para ENS (auditorias de seguridad) muy escueta (inicio de proyecto y auditoría). Detalla de forma más extensa en la auditoria sobre protección de datos. No tiene en cuenta la especificidad de sanidad. La valoración es escaso.

TECNOLOGÍAS PLEXUS, S.L.:

Hace una propuesta de valor, proporcionando la herramienta Risk4All para dar soporte a la implementación y mantenimiento de los sistemas de gestión de la seguridad y privacidad, análisis de riesgos, cumplimiento del RGPD, contexto del riesgo, planes de acción, identificación de activos, plan de mejora continua. La herramienta se integra con diferentes herramientas del CCN: PILAR, INES, LUCIA, etc...La metodología para la auditoría de protección de datos es amplia y con fases claras, aunque no aporta posible planificación y contempla un solapamiento con proveedor saliente que no existe. Respecto la auditoría de ENS tiene en cuenta la especificidad de sanidad y sigue las recomendaciones del perfil de cumplimiento especifico de salud (PEC SALUD CCN). Detalla cada fase de adecuación. Busca sinergias entre auditorías ENS y protección de datos. La valoración es excelente.

TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.:

Aporta un detalle amplio del contexto de la necesidad de esta oficina de auditoria interna en otros sectores, junto con una visión integradora de las diferentes auditorias proponiendo un plan de proyecto común. Indica que dispone de la experiencia como empresa que da servicios de seguridad y que cuenta con empresa especializada Govertis, empresa experta en gobierno, riesgo y cumplimiento (GRC) dentro del grupo empresarial que colabora con CCN.

Para la gestión del proyecto propone empleo metodología PMBOK y utilizar herramientas CCN (PILAR y metodología MAGERIT). La descripción y enfoque que realiza es muy generalista, aplicable a cualquier sector, sin aportar indicadores de media adicionales al PPT.

En la auditoria de protección de datos, delimita primero los trabajos a desarrollar y luego establece dos fases de desarrollo (preparación y ejecución, en esta olvida incluir al SUMMA112), con lo que no queda sistematizado su desarrollo.

Respecto a la auditoria ENS (seguridad) describe tareas a realizar y luego describe fases de desarrollo, indicando que tareas corresponden a cada fase. En las normas a utilizar para la auditoria no menciona expresamente la relativa al PCE SALUD, aunque se refiere de forma genérica a otras guías CCN STIC, no aporta herramientas adicionales.
No propone herramientas para la gestión, ni formula más aportaciones de valor. La valoración suficiente.

9.2.1.2. Gestión del Proyecto (hasta 16 puntos)

Se valorará la planificación de las actividades descritas en el pliego con los cronogramas, fases, tareas, recursos e hitos correspondientes.
Se valorará el Control y Seguimiento del Proyecto, Metodologías de actuación y las medidas de control y seguimiento dispuestas para el proyecto. Bueno.

Regla de puntuación:

- EXCELENTE (100%): Máximo nivel de adecuación de la metodología y máximo nivel de detalle de las medidas de control y seguimiento dispuestas para el proyecto.

- BUENO (75%): Buen nivel de adecuación de la metodología y buen nivel de detalle de las medidas de control y seguimiento dispuestas para el proyecto.

- SUFICIENTE (50%): Suficiente nivel de adecuación de la metodología y adecuado nivel de detalle de las medidas de control y seguimiento dispuestas para el proyecto.

- ESCASO (0%): Insuficiente nivel de adecuación de la metodología y escaso nivel de detalle de las medidas de control y seguimiento dispuestas para el proyecto.

9.2.1.2. Gestión del Proyecto (máx. 16 puntos)	
EMPRESA	PUNTUACIÓN
ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.	12
AYESA ADVANCED TECHNOLOGIES, S.A.	12
EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.	12
FUJITSU TECHNOLOGY SOLUTIONS, S.A.	12
INETUM ESPAÑA, S.A.	8
LAMBDA SEC S.L.	8
MNEMO EVOLUTION & INTEGRATION SERVICES S.A	8
PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.	8
PROCESIA PROYECTOS Y SERVICIOS, S.L.	12
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0
TECNOLOGÍAS PLEXUS, S.L.	12
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.	0

ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.:
Propone un modelo de relación en tres niveles (estratégico, táctico y operativo) donde detalla, en cada caso, participantes y tareas. Describe fases del servicio de forma amplia y planifica temporalmente el desarrollo de auditorías de protección de datos o adecuación al ENS, sin entrar en detalles. La valoración es bueno.

AYESA ADVANCED TECHNOLOGIES, S.A.:
La gestión del proyecto tiene como referencia el marco PMBoK. En la propuesta detalla las fases con los objetivos de cada una de ellas. Llegando hasta a definir los procedimientos que tendrá la gestión del servicio, y un breve resumen de qué contendrán los mismos, con el objetivo que persiguen.
Complementan la oferta con refuerzos de unidades internas de la compañía (por ejemplo, oficina de calidad corporativa y centros de competencias)

Detalla un modelo de relación con dos niveles: operativo y estratégico, donde ya define los comités que habrá, periodicidad, miembros, relación con otros agentes implicados e incluso entregables. Un comité director mensual y un comité operativo quincenal o semanal.
Propone un plan de la calidad basado en ISO 9001 y el modelo CMMI
La valoración es bueno.

EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.:
Diseña diversos comités para el modelo de relación a diferentes niveles (estratégico/ mensual, operativo/semanal y táctico/a demanda) detallando el objetivo de cada comité, com`posición y tareas. Contempla un seguimiento del servicio basado en cuadro de mando integral e informes específicos monitorizando los ANS. Se propone la creación del plan de calidad basado en ISO 9001. Se propone un plan de gestión de riesgos, con una base inicial en posibles riesgos. No propone metodología especifica ni formula aportaciones en materia de protección de datos. La valoración es bueno.

FUJITSU TECHNOLOGY SOLUTIONS, S.A.:
Propone la utilización de metodología PMI, SCRUM e ITIL, para establecer indicadores clave de rendimiento los factores críticos de éxito. Propone un comité de dirección y otro de seguimiento, proponiendo estructura de informes y cuadros de mando para ambos. Define entregables y realiza amplia descripción de indicadores claves de rendimiento.

Proporciona de manera coherente y detallada una planificación con las diferentes fases, sus etapas, entregables, y metodología a utilizar. Adaptando un enfoque práctico de SCRUM a las actividades a realizar, para poder ir teniendo entregables con pequeñas iteraciones y sin desviaciones en lo esperado y lo entregado.

Para las auditorías propone la utilización de la metodología MAGERIT, para análisis de reiesgos, y la herramienta PILAR (ambas herramientas CCN). El equipo lo forman expertos en GRC (gobierno riesgo y conformidad) y ofrece respaldo de grupo expertos para asesorar en esta materia. La valoración es bueno.

INETUM ESPAÑA, S.A.:
Articula un modelo de relación basado en cuatro niveles, donde especifica intervinientes en cada nivel y detalla poco la información sobre los entregables a realizar. No considera a C. Sanidad/SERMAS. Detalla equipo de trabajo y sus funciones así como el flujo de trabajo interno. Además, formaliza el proceso con el establecimiento de una serie de planes (capacidad, disponibilidad, continuidad ygestión de riesgos). No describe metodología a utilizar, ni detalla desarrollo de auditorías. La valoración es suficiente.

LAMBDA SEC S.L.:
Configura el proyecto como una oficina técnica que coordina la ejecución de las auditorias y acumula la experiencia y conocimiento extraído de estas. Establece fases de desarrollo, e identifica áreas de enfoque, define entregables (informe auditoría, acciones correctivas, actualización procedimientos y registro evidencias). Propone una metodología teniendo en cuenta PMI, SCRUM e ITIL. Establece un plan de auditoria anual, pero no aporta herramientas específicas. Propone mejoras de calidad a través de la revisión de los ANS y aporta ejemplos de informe de auditoría y no formula propuestas en materia de protección de datos. La valoración es suficiente.

PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.:
Propone un modelo de seguimiento a tres niveles (estratégico, táctico y operativo) con sus comités y empleo de metodologías agiles y metodología propia. Buena descripción de los contenidos de cada comité y de las partes implicadas. Propone el empleo de metodologías ágiles y metodología propia. Realiza una planificación de las auditorías de protección de datos y adecuación ENS coherente. Además, propone un plan de calidad y continuidad y otro de gestión de riesgos. La calificación es suficiente.

PROCESIA PROYECTOS Y SERVICIOS, S.L.:
Contiene una planificación detallada de las auditorias de seguridad ENS y protección de datos. Contempla la relación con SERMAS y C. Sanidad. En el modelo de relación contempla comité director, operativo y de seguimiento con una buena descripción de los diferentes interesados. Proponen acciones de mejora continua y la evolución de las diferentes métricas de seguimiento adicional a los ANS establecidos para medir la calidad del servicio. La valoración es buena.

MNEMO EVOLUTION & INTEGRATION SERVICES S.A.
Articula correctamente el modelo de gestión del servicio, proponiendo la utilización de metodología ITIL, PMOBK y COBIT para definir modelo operativo, de relación, informe y mecanismos de control, monitorizando ANS y proponiendo nuevos indicadores (solidarios, auditoria y satisfacción usuarios). Establece como mecanismo de control un comité director y operativo, donde no detalla entregables, pero si funciones y participantes. Propone definir distintos tipos de informes, y define de forma amplia las actividades en la planificación del servicio. Es una propuesta generalista que no incluye los objetivos que persigue el lote 1. No concreta al ámbito sanitario, ni aporta propuesta de valor añadido. La valoración es suficiente.

S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.:
Hace un planteamiento metodológico muy resumido para las auditorias de seguridad del ENS y amplia descripción en la relativas a protección de datos. No concreta actividades específicas en el ámbito sanitario. La valoración es escaso.

TECNOLOGÍAS PLEXUS, S.L.:

La propuesta de servicio es clara, concisa y coherente. Haciendo un desglose por las tres grandes fases que indica el pliego. Cada una de ellas con una serie de actividades, responsables asignados, calendario, entregables, análisis de riesgos de cada fase.

Proponen indicadores complementarios de los ANS y control de riesgos y su cuantificación en cada fase.

Como metodología proponen ITIL para la gestión del servicio y PMBOK para la gestión del proyecto. Como propuesta de valor aportan un grupo de expertos de la empresa y la posibilidad de un grupo de respaldo ante picos de trabajo. Confunde en el modelo de relación las entidades intervinientes (SERMAS, DGSD y las Consejerías de Sanidad y Digitalización). La valoración es buena.

TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.:

Realiza una descripción generalista de la gestión del proyecto, adolece de falta de concreción y adaptación al entorno sanitario. Propone utilizar indicadores para medir el desarrollo del servicio, sin definir posibles indicadores. Tampoco aporta metodología especifica ni herramientas. La valoración es escasa.

CONCLUSIÓN

En consecuencia, la valoración obtenida por la oferta analizada de las empresas presentadas, en el marco de la licitación del expediente A/SER-047045/2023 para criterios de valoración técnicos, según juicio de valor, es la siguiente:

LOTE 1						
EMPRESA	Criterios cuya cuantificación depende de un juicio de valor para el Lote 1 (máx. 36 puntos)					PUNTUACIÓN TOTAL CRITERIOS JUICIO DE VALOR
	9.1.1. Propuesta y enfoque	9.1.2. Otro servicio de	9.1.3. Plan de Formaci	9.1.4. Plan de concien	9.1.5. Cumplimiento	
CIPHERBIT, S.L.U.	16	5	6	4	5	36
IZERTIS, S.A.	12	2,5	3	2	3,75	23,25
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	0	0	0	0	0	0
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0	0	0	3	2,5	5,5
TECNOLOGÍAS PLEXUS, S.L.	12	2,5	3	3	2,5	23

LOTE 2			
EMPRESA	Criterios cuya cuantificación depende de un juicio de valor para el Lote 1 (máx. 36 puntos)		PUNTUACIÓN TOTAL CRITERIOS JUICIO DE VALOR
	Propuesta de alcance, metodología y tipología de las auditorías (máx. 36 puntos)		
	9.2.1.1. Visión global e integradora. Metodología, Descripción y Contenido de los Trabajos (máx. 20 puntos)	9.2.1.2. Gestión del Proyecto (máx. 16 puntos)	
ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.	10	12	22
AYESA ADVANCED TECHNOLOGIES, S.A.	10	12	22
EY TRANSFORMA SERVICIOS DE CONSULTORIA, S.L.	15	12	27
FUJITSU TECHNOLOGY SOLUTIONS, S.A.	15	12	27
INETUM ESPAÑA, S.A.	10	8	18
LAMBDA SEC S.L.	0	8	8
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.	10	8	18
PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.	10	8	18
PROCESIA PROYECTOS Y SERVICIOS, S.L.	15	12	27
S2 GRUPOSOLUCIONES DE SEGURIDAD, S.L.U.	0	0	0
TECNOLOGÍAS PLEXUS, S.L.	20	12	32
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.U.	10	0	10

Lo cual se indica a los efectos oportunos.

Madrid,
EL SUBDIRECTOR GENERAL DE INNOVACIÓN
Y SOLUCIONES ASISTENCIALES

Firmado digitalmente por: SÁNCHEZ PRIETO FRANCISCO LUIS
Fecha: 2024.06.03 14:58

[redacted]