GOBIERNO DE ARAGON
Departamento de Ciencia, Universidad y Sociedad del Conocimiento

Unión Europea

Aragonesa de Servicios Telemáticos

Avenida de Ranillas, 3 A, 3ª planta
50071 Zaragoza (Zaragoza)

Programa Operativo Fondo Europeo de Desarrollo Regional Aragón 2014-2020 o 2021-2027

Financiado como parte de la respuesta de la Unión a la pandemia de COVID-19

Construyendo Europa desde Aragón

Expediente número: **AST_2022_004**

INFORME TÉCNICO DE VALORACIÓN PARA LA CONTRATACIÓN DEL ACUERDO MARCO PARA LA PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD CON DESTINO A LOS DEPARTAMENTOS DE LA ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN Y SUS ORGANISMOS PÚBLICOS DEPENDIENTES

Unión Europea

Contenido

1. Antecedentes

Con fecha 19 de octubre de 2021 se aprueba el expediente de contratación del "ACUERDO MARCO PARA LA PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD CON DESTINO A LOS DEPARTAMENTOS DE LA ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN Y SUS ORGANISMOS PÚBLICOS DEPENDIENTES", con número de expediente AST_2022_004, a adjudicar por procedimiento abierto, sujeto a regulación armonizada y varios criterios de adjudicación.

Con fecha 22 de octubre de 2021 se publica el expediente en la Plataforma de Contratación del Sector Público. El plazo máximo de presentación de proposiciones fue el 25 de noviembre de 2021.

Enlace de la licitación:

https://contrataciondelestado.es/wps/portal/!ut/p/b0/DcoxCoAwDADABznEToLg4NBVFEFtFwlpkGCsDqX9vh0PDjwc4CNmuTDJG1GrXWD-VOLdB06oyqcKSUKqAXbw4CXYrOBcoSkbMs24HsvW7rZTN5dhgO95xh-qKQYs/

Concluido el plazo de presentación establecido, con fecha 13 de diciembre de 2021 tiene lugar la apertura electrónica de los Sobres B, ("PROPUESTA SUJETA A EVALUACIÓN PREVIA"), de las empresas admitidas a la licitación, tras verificar la mesa de contratación la documentación administrativa presentada por los licitadores, tras las subsanaciones requeridas, en el denominado Sobre nº A, siendo las empresas admitidas las siguientes:

1. UTE ACCENTURE, S.L. Y ECIX GROUP S.L.
2. CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)
3. INETUM
4. NUNSYS, S.L.
5. OESÍA NETWORKS, S. L
6. SAYTEL SERVICIOS INFORMÁTICOS S.A
7. SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.
8. TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

El presente informe hace referencia al contenido de las ofertas sujetas a evaluación previa presentadas por dichos licitadores en el SOBRE B, las cuales se ajustan todas estrictamente al índice establecido en el Pliego de Prescripciones Técnicas.

2. Procedimiento de valoración

El equipo de valoración técnica está formado por personal de la Dirección de Tecnología y Sistemas de Aragonesa de Servicios Telemáticos:

1. Mª Eugenia Pamplona Falomir – Técnico de Sistemas - Área Seguridad
2. Ignacio Perez Helguera – Responsable de Área de Seguridad
3. Óscar Torrero Ladrero – Director de Tecnología y Sistemas

Los criterios de valoración a aplicar son los que se indicaban en el Anexo VII - Criterios de adjudicación subjetivos sujetos a evaluación previa (Sobre B) del PCAP. Dichos criterios son los expuestos en el apartado nº 3 de este informe.

Las valoraciones de este informe son el resultado del consenso de los técnicos mediante la puesta en común de las valoraciones y apreciaciones individuales.

El apartado nº 4 del presente informe contiene de forma resumida, para cada uno de los criterios valorados, los aspectos más destacados de cada oferta y que han sido considerados a la hora de establecer las puntuaciones de cada licitador. Se trata de aspectos tanto positivos como negativos que han sido valorados teniendo en cuenta su importancia relativa de cara a la prestación del servicio.

El presente informe ha sido validado por todo el equipo de valoración, considerando que las puntuaciones finales reflejan adecuadamente la calidad global de las ofertas técnicas presentadas y las diferencias entre ellas.

Debido a las cláusulas de confidencialidad que los licitadores han invocado en cada una de sus propuestas así como a la debida reserva que las cuestiones de ciberseguridad requieren, el informe de valoración no entra a detallar características de dichas ofertas sino enfoques generales y omite todas aquellas consideraciones que o bien se han marcado claramente como confidenciales o si no se ha hecho mención expresa sino general a la confidencialidad, el equipo de valoración ha considerado que deberían ser omitidas, en aras a preservar detalles de la infraestructura y de las configuraciones y productos a utilizar. No obstante, al publicarse el contenido de este informe de valoración, no podemos sino hacer traslado de las apreciaciones y consideraciones que han motivado la puntuación en cada ítem que a continuación se traslada.

3. Criterios de valoración

En el **Anexo nº VII del Pliego de Cláusulas Administrativas Particulares (PCAP)** se establecen los Criterios de adjudicación subjetivos sujetos a evaluación previa (Sobre B) hasta una puntuación máxima de 44 **puntos**.

La valoración de cada uno de dichos criterios se realiza en base a los distintos apartados contenidos en el documento de la oferta presentada, según los puntos del índice establecido en el **apartado 10.2 Contenido de las ofertas del Pliego de Prescripciones Técnicas (PPT)**.

Las ofertas han omitido cualquier dato en el SOBRE B que esté sujeto a evaluación posterior y que por tanto deba ir incluido dentro del SOBRE C.

A continuación, se detallan los aspectos técnicos solicitados en la oferta y que son objeto de valoración en este informe.

CRITERIOS DE ADJUDICACIÓN		PUNTUACIÓN MÁXIMA
1. Calidad del personal que se adscribirá a la ejecución de los trabajos derivados		**14**
Se valorará la cualificación del personal que el licitador se compromete a adscribir a la ejecución de los trabajos que se deriven, adicional a los criterios de solvencia. Se tendrán en cuenta los siguientes aspectos: a) Composición por perfiles y nivel de conocimientos y experiencia del personal que se compromete a aportar a la ejecución de los trabajos a medida que se vayan demandando, en relación al objeto y al contexto del presente acuerdo marco, con especial referencia a la cualificación de los perfiles especialistas. b) Experiencia y conocimientos que se aportarán en el ámbito particular de las administraciones públicas y más concretamente en el ámbito de las soluciones de desarrollo de servicios digitales. DOCUMENTACIÓN: Según el apartado 10.2.1 del Pliego de Prescripciones Técnicas (PPT)		
2. Gobernanza de la Ciberseguridad		**12**
Se valorará una propuesta de Gobernanza de la Ciberseguridad, para el entorno descrito en el pliego como modelo operativo propuesto (organización y gestión) para cubrir los servicios demandados, así como el modelo propuesto de interacción entre los distintos actores, tanto internos al Gobierno de Aragón, como externos: integradores o proveedores. Se tendrá en cuenta el modelo propuesto para la provisión de los distintos servicios: • Gestión global del servicio. • Modelo de relación previsto entre los distintos actores • Gestión del conocimiento. DOCUMENTACIÓN: Según el apartado 10.2.2 del Pliego de Prescripciones Técnicas (PPT)		
3. Metodologías y herramientas		**10**
Se valorará el grado en que resultarán adecuadas, para las necesidades y objetivos planteados, las metodologías particulares que el licitador propone aplicar en cada caso a la hora de ejecutar los distintos proyectos o servicios que puedan derivarse dentro del contexto indicado en el presente pliego, teniendo en cuenta las distintas tipologías de proyectos. Se tendrán en cuenta los siguientes aspectos:		

a) Metodologías específicas a utilizar. b) Herramientas para la automatización y la gestión de los activos a proteger c) Puesta a disposición del servicio de otras herramientas y medios adicionales a los requeridos que incidan positivamente en la prestación del servicio, como por ejemplo la puesta a disposición, en los casos que lo requieran, de herramientas, cuadros de mando o cualquier otra herramienta que facilite el seguimiento y la consecución de los objetivos previstos. DOCUMENTACIÓN: Según el apartado 10.2.3 del Pliego de Prescripciones Técnicas (PPT)		
4. Arranque y devolución del servicio		**4**
Se valorará el grado en que resultarán adecuados, para las necesidades y objetivos planteados, los planteamientos del licitador para cada una de las fases por las que atravesará el servicio, ya sea con anterioridad o posterioridad a la fase regular o por las necesidades que puedan producirse a lo largo de la misma. En la medida en que apliquen al contexto particular del lote de que se trate, se tendrán en cuenta los siguientes aspectos: a) Arranque del servicio. Medidas preparatorias y compromisos que tiene previsto adoptar el licitador tras la firma del acuerdo marco de cara a poder asumir la responsabilidad del servicio en los plazos previstos y garantizar, en su caso, su continuidad con el mínimo impacto tras el arranque del mismo. Planificación, organización y equipo involucrado (indicando si se trata de recursos específicos de la transición o destinados al servicio) para asegurar la transferencia de conocimiento sobre los sistemas, aplicaciones, procesos y herramientas. Asimismo, medidas y compromisos que el licitador tiene previsto adoptar en fase regular para el caso de la incorporación de nuevas soluciones al servicio en el menor plazo posible. b) Devolución del servicio. Medidas y compromisos que el licitador tiene previsto adoptar a lo largo y al final del servicio para facilitar la devolución de la responsabilidad del mismo a AST o a quien ésta determine en los plazos previstos. Medidas y compromisos que el licitador tiene previsto adoptar en fase regular en el caso de devolución de soluciones al cliente, o a quien este determine, o de su traspaso a otro proveedor, en el menor plazo posible. DOCUMENTACIÓN: Según el apartado 10.2.4 y 10.2.5 del Pliego de Prescripciones Técnicas (PPT)		
5. Valores y aptitudes		**4**
Se valorará la demostración de los valores y aptitudes que el licitador se compromete a aportar para el cumplimiento de los objetivos y necesidades planteados y para hacer frente al contexto particular de la Administración de Aragón, teniendo en cuenta asimismo el ámbito concreto del lote al que se opte (compromiso, innovación, flexibilidad, proactividad, capacidad, etc.). Se tendrán en cuenta, entre otros, los siguientes aspectos: a) La proactividad y el compromiso con la mejora continua del servicio. Propuestas innovadoras que puedan suponer una mejora de los niveles de servicio ofrecidos, una mejora de la eficiencia en la realización de las actividades y/o una reducción de costes para la administración. b) La flexibilidad y capacidad para adaptarse a las condiciones cambiantes derivadas de la propia dinámica de las actividades llevadas a cabo desde la Administración. c) La aptitud para hacer frente a cualquier circunstancia, planificada o sobrevenida, que pueda surgir por el simple devenir del desarrollo de las actividades. DOCUMENTACIÓN: Según el apartado 10.2.6 del Pliego de Prescripciones Técnicas (PPT)		
PUNTUACIÓN TOTAL		**44**

4. Detalle y valoración de las ofertas

4.1. Calidad del personal que se adscribirá a la ejecución de los trabajos derivados

Criterio	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Calidad del personal que se adscribirá a la ejecución de los trabajos derivados	9	4	9	6	3	11,5	11	10

a) UTE ACCENTURE, S.L. Y ECIX GROUP S.L.

Se indican los perfiles del compromiso de adscripción de medios obligatorio, lo que no es objeto de valoración en este apartado, por lo que resulta la propuesta algo confusa. Se añaden otra serie de perfiles que sí, son objeto de valoración. Estos perfiles adicionales, aportan un conocimiento amplio de varios aspectos concernientes a la seguridad de la información en varios aspectos significativos, por ejemplo, las capacidadse en DevSecOps, con tecnologías de contenerización, hacking ético, SIEM, informática forense, evaluación de riesgos, Seguridad Cloud, gestión de vulnerabilidades, etc. Los perfiles adicionales son personal experto en varios ámbitos con experiencia en entornos complejos como el descrito en el pliego de prescripciones técnicas. No obstante, se echa a faltar algún perfil más ligado a cuestiones regulatorias o de cumplimiento

Existe una clara descripción del modelo operativo propuesto. Se indican fases y responsabilidades en la ejecución del contrato. No termina de entenderse la propuesta de ajuste de SLA, ya que podría dar a entender que estos compromisos no son firmes, sino volubles, cosa que no es lo que se determina en el pliego de prescripciones técnicas.

b) CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)

La estructura de la oferta no permite discernir ningun perfil adicional especifico en el que poder valorar el nivel de conocimiento y experiencia adicional, no obstante, si que hay que hacer constar que en el apartado se muestra un gran conocimiento con respecto al ambito de las administraciones publicas en servicios de ciberseguridad

c) INETUM

Existe una clara descripción del modelo operativo propuesto, con ciertos perfiles, pero no termina de indicarse de manera clara los perfiles básicos de los adicionales. La compañía cuenta con certificación tanto en metodologías como en productos y fabricantes de seguridad que asegura una correcta prestación del servicio y capacidad para llevarlo a cabo. Asi como experiencia concreta en contratos de ciberseguridad en el ambito de las administraciones publicas. La capacidad de la compañía está claramente indicada en cuanto a capacidad profesional como de especialistas. Se ponen de manifiesto profesionales de diferentes áreas de especialización para evidenciar su capacidad en los diferentes ambitos en los que se puede desenvolver el contrato. Se indican fases y responsabilidades en la ejecución del contrato

d) NUNSYS, S.L.

No queda claro cuales son los perfiles adicionales y cuales estan adscritos al servicio. Los perfiles dentotan capacidad técnica, pero carencia en certificaciones que avalen el conocimiento descrito. La relación de actividades en cada puesto ejercido es confusa.

Los proyectos de ciberseguridad detallados son escasos y acotados unicamente a una técnologia. No se muestra evidencia de conocimiento especifico de trabajo con otras administraciones públicas

e) OESÍA NETWORKS, S. L

Dada la estructura de la oferta, resulta complicado discernir si los perfiles indicados son adicionales a la adscripción de medios y de solvencia indicados para otro tipo de cuestiones dentro del contrato. A nivel global de perfiles ofrecidos OESIA está aportando personal con más experiencia de la solicitada superando de 3 años a 6 años tanto en perfiles senior como junior, pero en contrapartida no ofrecen certificaciones de fabricantes ni experiencia en herramientas específicas lo que penaliza ante implantaciones de herramientas de seguridad

Dentro de los perfiles indicados en este apartado, que como hemos indicado, no aclara si es adicional, se ofrece un Especialista de Seguridad dirigido a administraciones públicas, pero no aparece desglosado dicho perfil. En el ámbito concreto de las soluciones de desarrollo de servicios digitales no aportan experiencia suficiente. No es clara la oferta en este punto.

f) SAYTEL SERVICIOS INFORMÁTICOS S.A

Incorpora perfiles adicionales con un enfoque más interno dentro de su pool de ciberseguridad. El personal adicional que la compañía indica cuenta con un alto grado de experiencia, con certificaciones

de fabricantes y experiencia en algunas herramientas, pero principalmente enfocadas a redes y comunicaciones.

A nivel global de perfiles ofrecidos disponen alto grado de experiencia, ofrecen variedad en certificaciones incluyendo algunas asociadas a herramientas corporativas como IBM QRadar, CCNA, CCNP, AD.

Aporta experiencia en otras AAPP como por ejemplo administraciones autonómicas de relevancia, entidades locales también muy importantes, aunque más orientadas al mantenimiento, provisión y administración de CPD's. Se relacionan también en el ámbito de las soluciones de desarrollo de servicios digitales dentro de servicios de salud y el ámbito universitario. Se aportan referencias en el diseño de infraestructura de red y seguridad, así como en sistema de monitorización de eventos e incidentes de seguridad respectivamente.

g) SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.

SIA está aportando personal adicional con nivel de conocimientos muy especializado, pero no deja clara la composición entre perfiles adicionales y aquellos obligatorios en la adscripción de medios.

A nivel global de perfiles ofrecidos la cantidad de Especialistas de Seguridad adicional ofertado es muy amplio, así como el nivel de conocimiento especializado y cualificación en cada materia/rama de ciberseguridad para dar cobertura a todas las líneas de trabajo del presente AM.

Los Jefes de Servicio aportan experiencia en administraciones públicas y la gestión de servicios de seguridad de los servicios de salud, así como otros servicios relacionados en ministerios y servicios de empleo. A nivel de especialistas hay experiencia en organismos como INCIBE. Concretamente en el ámbito de las soluciones de desarrollo de servicios digitales dentro de alguna entidad local de relevancia.

h) TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

Presenta una clara y detallada propuesta de modelo operativo alienada con los objetivos del pliego presentado. Se indica a detalle protocolos y procedimientos de actuación ante las situaciones normales que se pudieran presentar a lo largo del contrato y, además, las posibles contingencias que surjan en momentos de contingencia, lo cual cobra relevancia por el tipo de servicio a prestar dentro del alcance del presente acuerdo marco. Clara identificación de riesgos y actuaciones para mitigarlos. Presenta perfiles adicionales, con capacidad y con cierta presencia de referencias en el sector público, no detallando las capacidades que luego enuncian como capacidades tanto en auditoria normativa, como en temas legales relacionados con la Seguridad de la información, así como en servicios de concienciación, formación y comunicación

4.2. Gobernanza Ciberseguridad

Criterio	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Gobernanza de la Ciberseguridad	9	10	8	0	9	10	7	8

a) UTE ACCENTURE, S.L. Y ECIX GROUP S.L.

Se propone un seguimiento de las metodologías del proveedor, alternativa a la planteada en el pliego, con una serie de actividades. Se propone la creación y el diseño de indicadores clave de riesgo y rendimiento, así como unas métricas de seguridad. Para los proyectos se propone una gestión analoga a la indicada en pliego, con una gestión ágil y con una carga de tareas de backlog. Se proponen una serie de métricas tipicas de gestión de proyectos. La gestión del conocimiento indicada, adolece de concreción, ya que no se indica como se gestionará realmente y si se utilizará alguna herramienta de soporte o como se hará extensible ese conocimiento al resto de actores involucrados.

b) CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)

La propuesta realizada propone una metodologia adecuada en la gestión global del servicio. Con una estructura clara y unas funciones definidas para cada tipo de rol. Con el compromiso especifido de dedicación total de perfiles ante los contratos derivados. Definiendo como adaptaran los procesos marcados por el SIG de AST a su propia gestión. Así como una estructura de soporte centralizada.

Indica la existencia de Director de Proyecto. Detalla las funciones y el perfil formativo minimo. Pero no queda claro el nivel jerarquico ni integración del mismo con la propia compañia licitadora. Se especifica que tiene una figura de apoyo llamada gestor del contrato para temas administrativos. Especifica las figuras de Jefe de proyectos de los contratos derivados del acuerdo marco, a las que tambien llama responsables de implantacion. Especifica que su asignacion es unicamente durante la implantación al servicio, quedando eso si vinculado de forma indirecta al mismo. Concretan su formación minima y sus tareas. Sin entrar a detalle en su encaje jerarquico dentro de la compañia licitadora, ni organización de la misma que pueda aportar valor. Se menciona la fiura del Coordinador técnico del servicio y sus funciones.

Especifica la voluntad y capacidad de interactuar con otros departamentos y organismos del Gobierno de Aragón. De igual forma especifica la voluntad y capacidad de interactuar con otras empresas proveedoras de servicios IT (MSP) afectadas por los proyectos resultantes, siendo el Coordinador Técnico el encargado de gestionar ese aspecto.

Se pone como hito la creación de un Plan de Adecuación e información de servicio al cliente articulado en fases donde se indican objetivos, perfiles involucrados, entregables y marcos temporales.

c) INETUM

Se plantea a alto nivel su participación en el comité de direccion y en el comité de seguimiento. Faltando definición en la forma.

Indica la existencia de un gestor del servicio equivalente al Responsable del Servicio solicitado por el pliego. No queda claro el nivel jerarquico ni integración del mismo con la propia compañia licitadora. Separa esa figura de la dirección del servicio indicando que es representante de la dirección del licitador, pero no se explica como interactua con los comites. Tambien aparece la figura del Responsable del Plan de Devolucion del Servicio. Pero no se describe mas alla de una linea, ni se le dan atribuciones ni se indica cual es la relación y/o diferencia con el responsable del servicio.

Se menciona la figura de Jefe de proyectos de los contratos derivados del acuerdo marco. Sin entrar a detalle en su encaje jerarquico dentro de la compañia licitadora, ni organización de la misma que pueda aportar valor.

Manifiesta su voluntad de interactuar con terceras partes, pero siempre bajo la mediación directa de AST. Lo que resta eficacia ante proyectos definidos.

Evalua la gestión del conocimiento como un elemento interno del personal que presta el servicio.

d) NUNSYS, S.L.

Modelo confuso y alejado a lo planteado en el pliego el que propone en su oferta el licitador. No queda claro quien es el responsable del Servicio por parte del licitador. Describe la existencia de dos oficinas de gestión de servicios (SMO) y de proyectos (PMO), cuyo personal adscrito se entiende que ejercitaran la función de Jefe de proyectos de los contratos derivados del acuerdo marco. No especifica capacidad, voluntad, ni metodo para adquirir, fomentar y transmitir el conocimiento

La propuesta realizada no describe su participación en el comité de direccion, comité de seguimiento marcado en el pliego. No especifica la voluntad y capacidad de interactuar con otros departamentos y organismos del Gobierno de Aragón; asi como tampoco con otras empresas proveedoras de servicios IT (MSP) afectadas por los proyectos resultantes.

e) OESÍA NETWORKS, S. L

Ofrecen una Oficina Técnica de Seguridad para gestión de todos proyectos de seguridad, cuadros e informes de control con un adecuado seguimiento. El modo en que ofrecen cada una de las líneas de trabajo del acuerdo marco es detallado y coherente, con especial atención en la línea de implantación de herramientas. De cara a la línea de gestión del servicio: Ofrecen un Comité interno de Ciberseguridad de cara a la estrategia de AST para soporte entre áreas y cumplimiento de normativa

vigente, pero se penaliza ya que esta información no aparece en la sección de Gobernanza sino en otros apartados de la oferta. Como valor adicional ofrecen servicios de asesoramiento para el cumplimiento del ENS.

La oferta muestra claramente el conocimiento interno de Áreas de AST y distribución de tareas por lo que el modelo de relación es coherente. Ofrece una matriz de tareas para identificar participantes de AST. El modelo de relación previsto lo asume el responsable del servicio. Además, como valor añadido plantea un Comité Transversal de CiberSeguridad

Para ello ofrece crear Base de datos del conocimiento y procedimientos para su alimentación, propia metodología en la gestión de flujos unido a la línea de un plan de formación continuo a sus empleados, pero su detalle no es elevado.

f) SAYTEL SERVICIOS INFORMÁTICOS S.A

Ofrece coordinar todo desde la Oficina de Seguridad con el Responsable del Servicio que controle contratos derivados, equipo asignados y facturación asociada. En contrapartida, no clarifica si el resto de recursos de la oficina planteada están incluidos o no. Ofrece modelo por cada una de las lineas de actuación con su documentación asociada y herramientas a emplear, así como dashboards por proyecto. De cara a la línea de gestión del servicio será liderada por el responsable del servicio que canalizará las peticiones de ofertas por parte de AST y generará los informes de servicio necesarios. Ofrecen gestion de riesgos de ciberseguridad y seguimientos e informes variados para una gestión detallada. Propone la definición de un Plan de Seguridad del servicio.

La relación se realiza a través de la Ofina de Seguridad, Comité Operativo de Seguridad. Ofrece Plan Capacitacion: Personas y repositorios.

g) SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.

El modelo de gestión del servicio presentado y el grado de claridad no es alto. No conocen situación a nivel normativo, plantean la elaboración de politica de ciberseguridad cuando AST ya dispone de una publicada, por otro lado, refuerzan la gestión con ampliación de los comités definidos en pliego. De cara a la línea de gestión del servicio ofrecen su propia metodología en la gestión de contratos derivados, pero no ofrece detalles de cómo abordar esa gestión.

Su propuesta de trabajar de forma coordinada y unificada no es detallada y no ofrece de forma clara el modelo de relación entre actores internos y externos.

Se acogen a las herramientas de gestión de AST, pero su propuesta no describe de forma clara este aspecto. Se penaliza además por no incorporar la información en un apartado dedicado como se exige en pliego.

h) TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

Se propone una metodología de comunicación y seguimiento habitual en este tipo de servicios, alineada con lo expresado en el pliego del acuerdo marco, detallando con claridad los mecanismos de seguimiento y control. Del mismo modo se presenta con claridad y detalles la relación entre los distintos actores. Indican un protocolo ante contingencias del servicio, tanto relacionadas con cuestiones de infraestructura como relacionadas con el componente humano. Identificación de los riesgos asociados, con una matriz de riesgos bastante completa. No se encuentran referencias a la gestión de conocimiento.

4.3. Metodologías y herramientas

Criterio	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Metodologías y Herramientas	10	10	8	3	10	8	10	10

a) UTE ACCENTURE, S.L. Y ECIX GROUP S.L.

Se parte de un modelo metodológico habitual basado en ITIL y norma ISO 20000 y se indica la metodología propia de la compañía, con alto detalle. Se realiza una analisis detallado de las herramientas de ciberseguridad descritas en el pliego, con profusión de detalles, analisis previos a la implementación, fases de consultoria, de implementación, mejora continua. Se añaden otro tipo de herramientas de ciberseguridad típicas en entornos complejos como el del licitador. Medologías claras y habituales. Claridad y acierto en la exposición de los objetivos. Foco en la automatización de todo lo posible, apoyándose en las capacidades de las herramientas descritas. La capacidad de la compañía se pone de manifiesto con los medios y capacidades descritas.

b) CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)

En lineas generales denota madurez en la puesta en practica de servicios equivalentes, proponiendo casos de uso concretos y formas de abordarlo. Aunque adolece de especificar mejor los marcos de

referencia utilizados mas alla de las guias CCN-STIC 800. Tambien se echa en falta una mayor definicion de los cuadros de mando propuestos.

Denotan un gran conocimiento y adecuación al ENS y de las guias CCN-STIC serie 800. Una gestión de servicios basada en ITIL. En cuanto a la respuesta a incidentes, si bien se destaca su pertenencia a csirt.es se echa en falta el marco de referencia usado en los IRP.

Plantea como estandares de seguridad ofensiva, analisis de vulnerabilidades y pentesting. CVSS, OWASP

Hay un extenso desglose de las herramientas de segurirdad utilizadas, puestas a disposición de AST.

Proporciona un maduro cuadro de mando propio: FARO para el descubrimiento y gestion de vulnerabilidades. Definicion de diversos casos de uso y tecnologia utilizada en cada caso, pero no como un servicio adicional, si no como idea de los posibles proyectos a acometer.

c) INETUM

Denota un conocimiento extenso en la ejecucion de proyetos. Le falta reforzar sus propuestas con certificaciones superadas.

Se mencionan las metodologias ISO 2000 (ITIL), ISO 9001 y CMMI. Pero no queda claro como es la integración de dichas metodologias en los procesos de la entidad licitadora en lo que respecta a este pliego.

Plantea un interesante mapeo de todos los proyectos bajo la ISO 27001 y ENS. Asi como analisis de riesgos con PILAR, mencionando las guias de securizacion del CCN-STIC

En cuanto a la respuesta a incidentes, se valora que pertenece a csirt.es. Especifica un seguimiento del cybersecurity framework NIST, se echa en falta la especificación de las guias (NIST) que son de aplicacion. No plantea estandares de seguridad ofensiva, analisis de vulnerabilidades y pentesting.

Como herramientas especificas se menciona PILAR, una de GRC, OpenVAS y luego herramientas de ofimaticas. Quedando el conjunto con una definición por debajo de lo esperado.

Se ofrece un cuadro de mandos propio de forma gratuita para el control de proyectos.

Proponen un sistema que relaciona las alertas detectadas con MITRE para ayudar a contestualizar e identificar las TTP de un ataque. Sin embargo, al no relacionar que herramienta de explotacion genera las alertas ni si es un servicio adicional o una herramietna dentro de otros servicios, no se puede tener en cuenta. Ya que el conocimiento de MITRE es un estandar conocido y sin embargo su correlación no resulta una tarea trivial como para entender que aplicaran la misma a cualquier ticket que les llegue.

Tambien propone workshops que, si bien son interesantes, en la practica no se diferencian de la tarea comercial y preventa general de cualquier prestador de servicios TIC. No habiendo reflejado que valor diferencial aportan las mismas

d) NUNSYS, S.L.

Se mencionan las metodologias ITIL, PMP, Scrum, PRINCE para la gestión de proyectos y servicios. Pero no se explica como interactuan entre ellas (PMP y PRINCE chocan sobre los mismos procesos con enfoques diferentes. Excepto para el apartado donde se hace mención a la metodología ITIL, no se realiza una definicion clara de sus procesos. Resulta confuso el modelo que desdice las certificaciones de la compañía tanto en ISO 9001 y como en ISO 2000, por lo tanto, orientada a procesos IT. Conocimiento demostrado en ENS e ISO 27001 (SGSI)

Hay menciones a leyes derogadas (LOPD, 1999). Asi como a estandares de continuidad anulados (UNE 71599), sin mencionar siquiera a las normas equivalentes actualizadas. No describe el marco de referencia usado en los IRP. No plantea estandares de seguridad ofensiva, analisis de vulnerabilidades y pentesting.

No describe ninguna herramienta para la automatización y la gestión de los activos a proteger

No describe cuadros de mando, herramientas o medios adicionales que sean de relevancia para el Acuerdo Marco

e) OESÍA NETWORKS, S. L

Aportan múltiples metodologías para las diferentes líneas de gestión PMBOK, ITIL, ISO/IEC 20000, ISO/IED 25000, ISTQB, ISO/IEC 27001, ENS, MAGERIT e ISO/IEC 22301 así como descripción de metodogías ante la gestión de incidentes de seguridad.

Enumeran múltiples herramientas de seguridad en líneas de actuación, pero no detallan si incorporan su implantación por lo que se valora solo el conocimiento que poseen en ellas. Como valor añadido destacar la realización de descubrimiento de activos a través de solución BloundHood+NMAP junto a explotación de las vulnerabilidades de los activos encontradas.

Ofrecen herramienta para elaborar cuadros de mando para seguimiento AM, proyectos, incidencias y peticiones (ANS). Ofrecen su SmartSOC para el tratamiento de ciberincidentes

f) SAYTEL SERVICIOS INFORMÁTICOS S.A

Metodologías ágiles como Scrum para gestión de proyectos derivados. Framework NIST y ENS para definición de controles y mecanismos de seguridad. Metodología propia para la línea de consultoría. No ofrecen metodologías de cara a la gestión de ciberincidentes.

Plantean soluciones para la automatización operativa de procedimientos y tecnología con un nivel de detalle adecuado, pero no aportan soluciones para la gestión de activos salvo la integración con las CMDBs existentes.

Ofrecen herramientas para elaborar cuadros de mando para seguimiento AM, proyectos, incidencias y peticiones asi como uno global de ciberseguridad. Ofrecen su Saytel-CSIRT para el tratamiento de ciberincidentes.

g) SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.

Se adaptan a las existentes en AST y adicionalmente ofrecen para gestión de servicios ITILv3, PRINCE2, COBIT y Lean TI, gestión de proyecto PMBOK y Metrica 3, gestión de vulnerabilidades, OSSTMM para la gestión de audiorias técnicas de sistemas, redes y servicios y OWASP para servicios web, MaGMa y MITRE para detección de incidentes. Ofrecen metodología propia para la respuesta ante incidentes basada en NIST y ENISA

Ofrecen más de 800 casos de uso para mejorar la detección de incidentes de seguridad. Realización de descubrimiento de activos a través de solución Qualys ofrecen el diseño de arquitecturas seguras. Ofrecen como valor añadido su conjunto de IOC's asociado a Threat Intelligence.

Ofrecen herramientas internas de SIA para gestión como por ejemplo SIA Reports para ofrecer diferentes vistas de información orientada a gestión, pone a disposición plantillas y formularios de documentación, pero deben utilizarse los corporativos de AST. El ofrecer un sistema de gestión interna de documentación no aporta valor para AST. Herramientas de reporting de indicadores de servicio

h) TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

Se propone una metodología propia y adaptada para los servicios que se deriven del acuerdo marco, según metodología ITIL. Se propone un equipo base de atención para derivar las necesidades que surjan a nivel de incidencias, peticiones o consultas. Se propone una oficina técnica para gestionar las herramientas y atención personalizada. Gestión de ANS, gestión del tiqueting mediante las herramientas indicadas en el pliego. Se ofrece la posibilidad de usar otras herramientas propias de

licitador con visión personalizada, para generar cuadros de mando, rendimiento, etc. así comom repositorio documental. Se hace referencia concreta a la implantación de herramientas de seguridad amplias y más allá de las indicadas en el pliego como referencia. Se especifica el proceso de implantación, así como metodologías habituales en este tipo de implantaciones. Se detallan fases, alcances y posibles escenarios con claridad. Se hace referencia a propuestas de mejora para idenficar y mitigar riesgos. Referencias normativas y planes de concienciación mediante la utilización de herramientas comunicativas.

4.4. Arranque y devolución del servicio

Criterio	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Arranque y Devolución del Servicio	3	3	3,5	0	3,5	3,5	3	3,5

a) UTE ACCENTURE, S.L. Y ECIX GROUP S.L.

Fase de arranque definida de manera clara, faltando algún compromiso específico adicional a los típicos en este tipo de arranque de contrato. Se echa en falta un cronograma que defina los tiempos de cada una de las fases.

Devolución del servicio correcta, pero algo parca. Sin cronograma, hitos, responsabilidades marcadas o compromisos adicionales a adoptar

b) CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)

Plan de arranque de servicio con coherencia y nivel de detalle. Establece fases del servicio en general, no tanto por contrato derivado si no como propuesta de acciones a tomar.

Plantea un Plan de Devolución con objetivos especificos y un cronograma basico.

c) INETUM

Plan de arranque de servicio con coherencia y nivel de detalle. Se establece un cronograma orientativo de comienzo, con diferentes tareas a abordar para comenzar con éxito el arranque del servicio.

Mencion de una figura Responsable del Plan de Devolucion, sin una definicion de relaciones clara. Por lo demas establece hitos claros en la devolucion, hacia AST o hacia otro proveedor asignado. Planteando las actividades necesarias de dimensionamiento eidentifaccion de RRHH, definicion de roles y responsabilidades, evaluacion de riesgos durante la fase y elaboracion de un plan de transferencia. Especificando el tipo de documentación objeto del traspaso y puntos a tener en cuenta.

d) NUNSYS, S.L.

No hay una minima definición de como gestionar el arranque al servicio. Tan solo que forma parte del responsable de produccion o resource manager la planificación y secuenciación de los servicios (proyectos), con alguna otra indicación.

No aparece ninguna mención al plan de devolución.

e) OESÍA NETWORKS, S. L

Plan de arranque de servicio con coherencia y nivel de detalle alto junto a un seguimiento adecuado donde plantea recursos específicos para la tranferencia de conocimiento con cronograma de hitos, tareas y duración.

Plan de devolución coherente con detalle de cronograma y planificación identificando procedimientos, actividades, hitos, plazos y responsables, pero no cada línea de actuación del acuerdo marco.

f) SAYTEL SERVICIOS INFORMÁTICOS S.A

Planteamiento de arraque de servicio con coherencia a dos fases, estableciendo cronograma de tareas y duración estimada de las fases controladas por Saytel unido a un plan de formación en paralelo para la adquisición del conocimiento y cuadros de mando para un seguimiento detallado de situación. En contrapartida no se definen los recursos implicados en el arranque por lo que se penaliza por ello

Ofrecen un Plan de devolución de servicio con duración estimada muy detallado y coherente con las tareas y acciones específicas por línea de actuación del acuerdo marco. Además, ofrece formación y sesiones de traspaso de conocimiento práctico realizando un test de madurez para evaluar la capacidad autónoma.

g) SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.

Arranque de servicio planteado con coherencia y planificación correcta con un Plan de puesta en marcha y un Plan de ejecución del proyecto. No ofrecen recursos específicos para la fase de arranque, por lo que se penaliza. No queda claro el Plan de Operación realizándose la misma mención en varios apartados en este aspecto lo que penaliza la puntuación, así como que no se plantea un cronograma ni estimación de plazos del arranque del servicio.

Ofrecen Plan de finalización del servicio en global pero no de cada línea de actuación, compromisos adecuados y con cierto nivel de detalle de tareas a abordar en el mismo indicando una estimación de los plazos y las tareas a abordar.

h) TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

Claro y detallado plan de arranque del servicio. Con fases, detalle de las tareas a realizar en cada fase, actores inclucrados, calendario, tareas, identificación de riesgos, mejoras, etc. Simplemente se echa en falta un cronograma tentativo donde se puedan ver las fases y tareas indicadas de manera más sencilla.

Detallado plan de devolución. Compromisos por parte del licitador, reflejados de manera clara. Metodología habitual en este tipo de procesos. Se vuelve a echar en falta un cronograma donde se establezcan la duración de las tareas indicadas, así como los actores involucrados

4.5. Valores y aptitudes

Criterio	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Valores y Actitudes	1,5	1,5	1,5	0	1,5	1,5	*1,5*	*2*

a) UTE ACCENTURE, S.L. Y ECIX GROUP S.L.

Compromiso, avalado por varias certificaciones en distintas normas y metodologías. Modelo de trabajo comprometido con la calidad y la mejora continua. No se hace referencia a ningún compromiso concreto con AST, como punto concreto de compromiso u objetivo a conseguir.

Se indica la capacidad para asumir desbordamientos. La disposición de personal experto. Marco metodológico marcado hacía la excelencia operativa.

Capacidad de la compañía para hacer frente a posibles circustancias, indicando capacidades y con un largo camino recorrido en cuestiones de ciberseguridad.

b) CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)

Menciona ejemplos de proactividad y compromiso. Sin terminar de aterrizar en que se materializa con respecto a AST o el AM.

Indica como lograr un frado de flexibilidad y capacidad. Sin terminar de aterrizar en que se materializa con respecto a AST o el AM.

c) INETUM

Menciona ejemplos de proactividad y compromiso. Sin terminar de aterrizar en que se materializa con respecto a AST o el AM.

Indica como lograr un frado de flexibilidad y capacidad. Sin terminar de aterrizar en que se materializa con respecto a AST o el AM.

d) NUNSYS, S.L.

No menciona los valores y aptitudes exigidos en el AM

e) OESÍA NETWORKS, S. L

En cuanto al compromiso, se indica que la empresa licitante pondrá a disposición los recursos necesarios para llevar a cabo las actividades demandas. Se propone en cuanto a proactividad, disponier del servicio 24x7 SmartSOC, acciones formativas, así como la creación y mantenimiento de bases de datos del conocimiento. En cuanto a la flexibilidad, no llama la atención ningún valor que aporte en este apartado.

Se indican recursos dentro del Centro de Competencias de OESIA, como parte de la capacidad, aunque existe poco detalle de qué se compone ese Centro

La aptitud para hacer frente a cualquier circunstancia, planificada o sobrevenida, que pueda surgir por el simple devenir del desarrollo de las actividades, no aparece reflejada en la oferta

f) SAYTEL SERVICIOS INFORMÁTICOS S.A

En cuanto a la proactividad indican que se comprometen a evitar la rotación, la formación continua y reasignación de recursos, los mismo que indican para la proactividad. En cuanto a flexibilidad, indican estar abiertos a modificar el modelo de servicio como equipo para responder a peticiones AST y su entorno.

Capacidad de adaptación para asegurar cumplimiento SLA ante cambios o tendencias, ofrenciendo un equipo anexo de especialistas de Ciberseguridad.

La aptitud para hacer frente a cualquier circunstancia, planificada o sobrevenida, que pueda surgir por el simple devenir del desarrollo de las actividades, no aparece reflejada en la oferta

g) SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U.

La proactividad y el compromiso con la mejora continua del servicio, así como propuestas innovadoras que puedan suponer una mejora de los niveles de servicio ofrecidos, una mejora de la eficiencia en la realización de las actividades y/o una reducción de costes para la administración, no aparece reflejado en la oferta.

En cuanto a la flexibilidad, se ofrecen mecanismos para abordar tareas planificables como no planificables, así como mecanismos de gestión de RRHH, retención y rotación

La aptitud para hacer frente a cualquier circunstancia, planificada o sobrevenida, que pueda surgir por el simple devenir del desarrollo de las actividades, no aparece reflejada en la oferta

h) TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA S.A.U

Se pone a disposición la capacidad de la compañía en aspectos de la ciberseguridad tales como el SOC, compromiso de poner a disposición sus capacidades como operador para facilitar la atención ante ataques que desde la capa de operador se puedan mitigar. Aspecto este muy valorable.

Gran capacidad de la compañía para poder aborar cualquier aspecto de los relacionados en el pliego, así como la capacidad y presencia de esta compañía en las distintas adminsitraciones públicas en materia de ciberseguridad lo que asegura las sinergias necesarias.

Capacidad de la compañía para hacer frente a posibles circustancias, indicando capacidades, certificaciones y con un largo camino recorrido en cuestiones de ciberseguridad.

5. Valoración Final

En base al detalle de las valoraciones del apartado anterior, el resultado final de la valoración es el siguiente:

Criterio	Máxima	ACCENT	CSA	INETUM	NUNSYS	OESIA	SAYTEL	SIA	TELEF
Calidad del personal que se adscribirá a la ejecución de los trabajos derivados	14	9	4	9	6	3	11,5	11	10
Gobernanza de la Ciberseguridad	12	9	10	8	0	9	10	7	8
Metodologías y herramientas	10	10	10	8	3	10	8	10	10
Arranque y devolución del servicio	4	3	3	3,5	0	3,5	3,5	3	3,5
Valores y aptitudes	4	1,5	1,5	1,5	0	1,5	1,5	1,5	2
TOTAL	**44**	**32,5**	**28,5**	**30**	**9**	**27**	**34,5**	**32,5**	**33,5**

Según las puntuaciones obtenidas, el orden de las ofertas es el siguiente:

1. **Licitador uno**

SAYTEL SERVICIOS INFORMÁTICOS S.A.…….....**34,5 puntos**

2. **Licitado dos**

TELEFÓNICA SOLUCIONES DE INFORMÁTICA.……..…....**33,5 puntos**

3. **Licitadores tres y cuatro**

UTE ACCENTURE, S.L. Y ECIX GROUP S.L. ..... **32,5 puntos**

SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U. ……..…....**32,5 puntos**

5. **Licitado cinco**

INETUM……..……..…….. **30 puntos**

6. **Licitador seis**

CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A. (CSA)…….....**28,5 puntos**

7. **Licitador siete**

OESÍA NETWORKS, S. L ……..……..…….....**27 puntos**

8. **Licitador ocho**

NUNSYS, S.L.……..... **9 puntos**

En Zaragoza, a fecha de firma electrónica.

Fdo. Mª Eugenia Pamplona Falomir – Técnico de Sistemas - Área Seguridad

Fdo. Ignacio Perez Helguera – Responsable de Área de Seguridad

Fdo. Óscar Torrero Ladrero – Director de Tecnología y Sistemas