ACTA DE CALIFICACIÓN SOBRE A

Licitación para la contratación del servicio de detección y respuesta a incidentes de ciberseguridad

En el domicilio social de TRABAJOS CATASTRALES, S.A.U. (en adelante, TRACASA GLOBAL), en Calle Cabárceno, nº 6º, siendo las 10.30 h del día 20 de octubre de 2022, según lo dispuesto en la estipulación 18 de las "Condiciones Reguladoras", se constituye la mesa de contratación con la asistencia de las personas que a continuación se relacionan:

- D. Emilio Rubio Cía, Responsable de Seguridad.
- Dña. Silvia Arteta Ahechu, Licenciada en Derecho.
- D. Joseba Itoiz Orzanco, Director financiero.

Seguidamente, a través de la Plataforma de Licitación Electrónica de Navarra (PLENA) y en virtud de la posibilidad otorgada por el artículo 97 LFCP se procede a la apertura del sobre A "Documentación general y propuesta de criterios cualitativos" presentado por las siguientes personas licitadoras:

- Integrated Technologies Systems, S.L. (ITS)
- One Esecurity (en adelante ONE)
- SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (en adelante SIA)

01. DOCUMENTACIÓN GENERAL

Todas las empresas han cumplimentado correctamente esta sección y se aceptan las tres proposiciones, continuando con el análisis de los criterios cualitativos.

02. CRITERIOS MEDIANTE JUICIO DE VALOR

Observado un defecto de imposible subsanación por tratarse de la inclusión de información relativa a criterios cuantificables mediante fórmulas en el sobre A, ONE queda automáticamente excluida del procedimiento, de conformidad con lo establecido en las condiciones reguladoras de este procedimiento de contratación.

En la descripción de los apartados a incluir en el sobre SOBRE B: PROPUESTA CRITERIOS CUANTIFICABLES MEDIANTE FÓRMULAS, en su apartado b) se especifica:

"Tiempo de respuesta en atención a incidentes:
Para la oferta de tiempo de respuesta en atención a incidentes se adjunta un modelo, Anexo III, donde la empresa licitadora deberá indicar en el cuadro el tiempo de respuesta en atención a incidentes."

Completado esto con la especificación recogida en el párrafo último de la cláusula 17, SOBRE A, donde se establece: ***"la inclusión de cualquier dato propio del sobre B determinará la inadmisión o exclusión de la proposición",*** podemos concluir afirmando que existen específicas indicaciones que implican, necesariamente, no facilitar datos relativos a tiempos de respuesta en atención a incidentes en el sobre A. Dado que la entidad ONE incluye en el apartado 7.1. de su oferta esta información, queda excluida del presente procedimiento continuándose el mismo con SIA y con ITS.

Con respecto a la puntuación de los criterios cualitativos de la oferta presentada, con una valoración máxima de 50 puntos y en donde se valoran los siguientes aspectos:

Equipos y medios necesarios: 10 puntos
Referido a la capacitación del personal técnico a disposición del servicio: experiencia, formación y conocimientos técnicos.

Metodología en la prestación de los servicios: 40 puntos
Se valorará la calidad de la propuesta presentada, su detalle técnico y funcional, de manera que permita obtener un alcance lo más completo posible de la propuesta presentada.

La puntuación final es la siguiente:

1. SIA

a) Equipos y medios necesarios: 10 puntos

Perfil	Experiencia acumulada en el perfil	SIA
DevOps / Ingeniería de ciberseguridad	Más de 10 años: 3 puntos Entre 5 y 10 años: 2 puntos Entre 2 y 5 años: 1 punto Menos de 2 años: 0 puntos	3
Operador	Más de 10 años: 3 puntos Entre 5 y 10 años: 2 puntos Entre 2 y 5 años: 1 punto Menos de 2 años: 0 puntos	3
Investigador	Más de 10 años: 2 puntos Entre 5 y 10 años: 1 puntos Entre 2 y 5 años: 0,5 puntos Menos de 2 años: 0 puntos	2
Responsable	Más de 10 años: 2 puntos Entre 5 y 10 años: 1 puntos Entre 2 y 5 años: 0,5 puntos Menos de 2 años: 0 puntos	2
TOTAL PUNTUACIÓN		**10**

En consecuencia, **la oferta presentada por SIA obtiene 10 puntos**

b) Metodología en la prestación de los servicios: 40 puntos

En este subservicio, se destacan las siguientes funcionalidades por Tracasa en lo referente a propuesta de solución y enfoque metodológico:

1. Solución SOCless: enfoca toda la solución SOC a la nube, ya que es un modelo de prestación del servicio 100% cloud.

Este diseño no considera nuestra política de infraestructuras, que es on premise.

No se especifica si se requerirá por Tracasa algún tipo de licenciamiento de plataformas cloud como Azure o AWS.

2. La propuesta metodológica de detección de incidentes basada en casos de uso se considera acertada por su simplicidad a la vez que efectividad.
3. El SIEM propuesto es Elastic. Se trata de un SIEM solvente, con multitud de integraciones, pero no ubicado en posiciones de liderazgo dentro de los cuadrantes Gartner, como de hecho se recoge en la propia página corporativa de Elastic.
4. La herramienta propuesta para Threat Hunting es propia de la empresa, LycaOn, no aportando más detalle de la misma y no aportando por lo tanto sus funcionalidades y potencial.
5. La planificación de los distintos servicios, recogida en la página 46, es muy clara y permite la obtención de hitos en breve espacio de tiempo.
6. No se incluye ningún detalle en el caso de un traspaso de servicios a otro proveedor una vez finalice este contrato.
7. Los logs de caso de uso se retienen durante 30 días, cifra inferior a la de otros licitadores.
8. En lo que se refiere al segundo de los servicios requeridos en el pliego, la propuesta de SIA se basa en nuestro Servicio de DFIR (Digital Forensics & Incident Response, por sus siglas en inglés) del que se incluyen 220 horas como bolsa de horas de servicio. Esta bolsa de horas es un 51% inferior a la bolsa presentada por el licitador con el mayor número de bolsa de horas ofertada.
9. El resto de los aspectos relativos a la respuesta a incidentes son satisfactorios.

En consecuencia, los productos y servicios ofertados dan una respuesta aceptable a los requisitos especificados en el pliego técnico.

En consecuencia, **la oferta presentada por SIA obtiene 25 puntos**

2. ITS

a) Equipos y medios necesarios: 10 puntos

Perfil	Experiencia acumulada en el perfil	ITS
DevOps / Ingeniería de ciberseguridad	Más de 10 años: 3 puntos Entre 5 y 10 años: 2 puntos Entre 2 y 5 años: 1 punto Menos de 2 años: 0 puntos	3
Operador	Más de 10 años: 3 puntos Entre 5 y 10 años: 2 puntos Entre 2 y 5 años: 1 punto Menos de 2 años: 0 puntos	2 (En las subsanaciones presentadas al sobre A, se indica "más de 5 años de experiencia" sin mayor especificación, por lo que se otorgan 2 puntos.)
Investigador	Más de 10 años: 2 puntos Entre 5 y 10 años: 1 puntos Entre 2 y 5 años: 0,5 puntos Menos de 2 años: 0 puntos	1 (En las subsanaciones presentadas al sobre A, se indica "más de 5 años de experiencia" sin mayor especificación, por lo que se otorga 1 puntos.)
Responsable	Más de 10 años: 2 puntos Entre 5 y 10 años: 1 puntos Entre 2 y 5 años: 0,5 puntos Menos de 2 años: 0 puntos	2
TOTAL PUNTUACIÓN		**8**

En consecuencia, **la oferta presentada por ITS obtiene 8 puntos**

b) <u>Metodología en la prestación de los servicios: 40 puntos</u>

En este subservicio, se destacan las siguientes funcionalidades por Tracasa en lo referente a propuesta de solución y enfoque metodológico:

1. Poder disponer de un SOC as a Service
2. Disponer de dicho SOCaaS en horario 24x7
3. Principales certificaciones del SOC (First, TF-CSIRT)
4. El servicio SOC incluye un ejercicio de Red Team (simulación de ataque) que nos permitirá certificar la calidad del servicio SOC recibido. Este servicio adicional de Red Team presenta un gran valor para Tracasa.
5. Sustentando en las principales bases metodológicas de la industria de la ciberseguridad con una amplia integración.
6. Uso de marcos ágiles de desarrollo como Scrum, coincidiendo así con los marcos metodológicos de Tracasa.
7. Facilitar una herramienta SIEM.
8. Que la herramienta SIEM escogida sea QRADAR, siendo la herramienta líder del mercado y que de forma sistemática es analizada por Gartner en sus informes como la aplicación SIEM de referencia.
9. Retención de los logs por cuatro meses.
10. Módulo UBA (User Behavior Analytics) que monitoriza a nivel de usuario o IP con lo cual se pueden crear políticas más capilares.
11. La consola de gestión CID360: La plataforma detecta, analiza y correlaciona indicadores entre archivos, usuarios, redes, dispositivos y puestos de trabajo. CID360 permite identificar amenazas desconocidas y que no han sido detectadas por los perímetros de protección, como ataques, ransomware y malware sin firmar, permitiendo su identificación y rápida eliminación. Se enfoca de esta forma sobre las amenazas potenciales con remediación automática y manual.
12. CiD360 utiliza un enfoque único para detectar amenazas, correlacionar y analizar indicadores entre archivos, usuarios, redes, dispositivos, identidades digitales y puesto de trabajo. Se integra en la infraestructura de seguridad existente, permitiendo a Tracasa una rápida capacidad y flexibilidad para dar una respuesta, neutralizando las amenazas desconocidas, las anomalías y el malware sin firmar que han pasado por alto las soluciones de detección existentes.
13. Eventos por segundo (EPS): incluyen 1.000 EPS en su dimensionamiento para el tenant dedicado a SIEM.
14. Incorporación de 10 casos de uso personalizados y orientados al negocio, además de los más de 400 casos de uso predefinidos por la herramienta.

15. Enfoque bajo tres niveles de inteligencia: operativa, táctica y estratégica.
16. Enfoque metodológico en la transición del servicio: la oferta incluye de forma detallada las prácticas metodológicas en el caso de que cambie el proveedor del servicio después de los 12 meses de contrato, lo cual se valora muy positivamente ya que proporciona a Tracasa flexibilidad y garantía de que al menos van a mantenerse los niveles de servicio.
17. Experiencia demostrada tanto en el sector IT como en la Administración Pública.
18. Bolsa de horas: llegando un montante total de 333 horas, siendo el licitador que presenta un mayor número de horas y siendo muy superior al resto de licitadores.
19. Disponer de recursos locales en Navarra, permitiendo de esta forma una prestación rápida del servicio que se valora muy positivamente dado que la rapidez es una variable fundamental en la recepción de este tipo de servicios.

En consecuencia, los productos y servicios ofertados dan una respuesta excelente a los requisitos especificados en el pliego técnico.

En consecuencia, **la oferta presentada por ITS obtiene 40 puntos**

A continuación, se recoge una tabla resumen de puntuación:

CRITERIO	SIA	ITS
Equipos y medios necesarios	10	8
Metodología en la prestación de los servicios	25	40
TOTAL	35	48

Asimismo, se deja constancia de que ninguno de los miembros integrantes de la mesa de contratación que suscribe el presente documento tiene interés financiero, económico o personal que pueda comprometer su imparcialidad e independencia en el procedimiento.

No habiendo más asuntos que tratar, siendo las 11h del día 14 de diciembre de 2022, se da por finalizada la calificación del sobre A.

Sarriguren, 14 de diciembre de 2022

Emilio Rubio Firmado digitalmente por Emilio Rubio Fecha: 2022.12.14 11:17:53 +01'00'	72820853R JOSEBA ITOIZ (R: B71280689) Firmado digitalmente por 72820853R JOSEBA ITOIZ (R: B71280689) Fecha: 2022.12.14 12:12:18 +01'00'	72805982B SILVIA ARTETA (R: A31112121) Firmado digitalmente por 72805982B SILVIA ARTETA (R: A31112121) Fecha: 2022.12.14 12:16:30 +01'00'
Emilio Rubio	Joseba Itoiz	Silvia Arteta
Responsable de Seguridad	Director Financiero	Área Jurídica