Servicio Integral de Ciberseguridad para RTVE (SIC23)

Informe Técnico

(Expediente S-06041-2022)

febrero 2023

Índice

1 Introducción

1.1 Objeto

El objeto del presente informe es la valoración de ofertas técnicas presentadas a la licitación del expediente **S-06041-2022 - Servicio Integral de Ciberseguridad SIC23**, consistente en la contratación de un servicio externo de Ciberseguridad que aúne las tareas relativas a la gestión de la ciberseguridad de ámbito corporativo, y que sea prestado por una empresa especializada y con medios y recursos altamente especializados y entrenados en las tecnologías de protección, supervisión y respuesta ante incidentes. La contratación de este servicio, permitiría acometer las acciones necesarias para dar respuesta a lo requerido por Comité de Ciberseguridad, en cuanto a coordinación de la Ciberseguridad Corporativa. La actividad de este servicio está orientada a contar con:

- Una Oficina Técnica de Ciberseguridad, que, entre otras funciones, intermedie entre el SOC y los admins de elementos de seguridad, realice servicios de reporting, consultoría e avanzada, etc.
- SIEM y SOC que monitoricen la actividad de los diversos componentes y servicios TIC para prevenir incidentes de ciberseguridad y, en el caso de que ocurran, detectarlos y ofrecer una respuesta rápida y adecuada.
- Servicios especializados que fundamentalmente integren fuentes al SIEM, den soporte avanzado a Ciberincidentes, etc.

1.2 Ofertas recibidas

Se han recibido ofertas de los proveedores:

Sistemas Informáticos Abiertos, S.A.

SOTHIS Servicios Tecnológicos, SLU

1.3 Ofertas Excluidas

Ninguna.

2 Valoración Técnica de las Ofertas

2.1 Criterios de Valoración Técnica.

Los criterios de valoración son los recogidos a tal efecto en el Pliego de Condiciones Generales.

2.2 Oferta de SISTEMAS INFORMÁTICOS ABIERTOS S.A.

Criterios técnicos sometidos a juicio de valor	Valor máx.	Valor SIA	Comentarios a Oferta de SIA
Solución Técnica y Metodología	15	8,63	
Servicios de la Oficina Técnica de Seguridad (OTS)	7,5	5,63	Respecto a adecuación al ENS y planes de mejora, se propone metodología genérica sin percibir aporte adicional orientado a RTVE. Incluye una propuesta de monitorización propia para adecuación al marco normativo. Respecto a soporte a ciberincidentes, se asiente a lo solicitado en el pliego sin percibir aporte de valor adicional para RTVE. Respecto a concienciación y formación se propone una metodología genérica sin aportar claramente ejemplos ni modelos como se solicita, salvo la cita a una herramienta para phishing ético. Respecto a bastionados, se propone la herramienta nessus sin coste y habla de guías de bastionado. Respecto a gestión de vulnerabilidades, se propone una metodología genérica y la herramienta tenable.io. Respecto al soporte de cumplimiento normativo, se propone una apreciable relación de actividades por normativa y se menciona el uso de la herramienta onetrust. Se propone un modelo de Gobierno Riesgo y Cumplimiento propio que incluye un modelo unificado de Controles sin aclarar explícitamente que dicho marco incluya todos los controles del ENS. Propone MARA como metodología propia de análisis de Riesgos. Propone Smartfense como herramienta de formación y concienciación basada en phishing y ransomware que se supone gratuita al no indicarlo en contra. Respecto a Gestión de capacidad y demanda, propone un modelo genérico de gestión de solicitudes segmentando por tipo de actividad sin mencionar el uso de la herramienta SIGO de RTVE.

Servicios Especializados	7,5	3,00	Propone un modelo genérico de gestión de soporte a Eventos, aunque en la participación de los eventos citados no queda claro el peso de la participación de SIA o Minsait. Se proponen pasos genéricos para evaluación de herramientas a partir del conocimiento de la situación actual si bien no cita detalle del soporte al despliegue de las propuestas, como se solicita. Respecto al ciclo de vida de los sistemas, se proponen pasos genéricos sin detallar herramientas orientadas a las necesidades de RTVE. Respecto a integraciones con el SIEM, se centra en el SIEM propuesto con integraciones nativas, sin especificar la posibilidad de mantenimiento de la infraestructura de sondas-SIEM actual en RTVE. Se hace un detalle notable de herramientas de apoyo y metodología. Respecto a auditoria y test de intrusión, no se identifica claramente oferta de valor orientada a RTVE. En el resto de aspectos no se aprecia más que asentimiento a los solicitado.
Equipo profesional	15	8,76	
Titulaciones	3,75	1,50	El equipo cumple la titulación requerida y solo alguno de los recursos presenta alguna titulación adicional de valor para el servicio.
Certificaciones adicionales de utilidad para el servicio	3,75	2,22	Sólo algúnos miembro presentan algún certificado adicional a lo solicitado de valor para el servicio.
Formación tecnológica aplicable al servicio	3,75	1,48	Solo algun miembro aporta formación adicional de valor para el servicio.
Experiencia adicional aplicable al servicio	3,75	3,56	Aunque el nivel de experiencia adicional es bueno, no todos los miembros cumplen con una experiencia adicional de valor para el servicio
Capacidades de SOC	15	8,30	

Metodología y procesos internos	3	1,40	Enumera de forma genérica procesos y actividades incluidas en el Servicio. Destaca la monitorización basada en Casos de Uso y la metodología Mitre y MaGma para conocimiento del origen de ataque. Cita light-response como entorno de actividades identificativas de incidente. Cita un proceso genérico de detección de amenazas externas almacenando información en herramienta DragonFly. Se proporciona DetectOne como portal de acceso a la información. Enumera de forma genérica procesos de gestión de proyectos (se solicita en el pliego detallar un servicio) sin hacer mención específica a gestión de capacidad y demanda.
Medios tecnológicos y herramientas	3	2,25	Se propone appliance de captura de eventos hacia el SIEM Mónica. Es notable el esfuerzo de adaptación al SIEM del CCN. Cita Dragonfly como herramienta de inteligencia de amenazas. Se hace enumeración notable de entregables, así como DetectOne como portal de gestión de servicios del SOC y numerosos entregables trimestrales, por alerta, de servicio de detección, etc. echando en falta orientados a las necesidades de RTVE, como pudiera ser informes segregados por Áreas Técnicas.

Flexibilidad para picos de trabajo no previstos	3	1,20	Dice únicamente ser flexible sin aportar detalle que permita juzgar idoneidad u orientación a las necesidades de RTVE.
Coordinación entre el equipo de personal in situ y remoto	3	1,20	Expone su organización y estructura de atención del SOC pero no queda totalmente clara la coordinación entre esos grupos de personal.
Homologaciones del SOC	3	2,25	En el resumen ejecutivo cita su certificación ENS Alto y Servicio Avanzado de Detección y respuesta sin quedar completamente claro qué homologaciones o certificaciones de valor para el servicio se poseen sobre las solicitadas .
Aspectos generales del servicio	5	2,20	
Plan de transición y recursos disponibles	2,5	1,00	Enumera un proceso genérico de actividades de transición citando la metodología shadowing para transferencia de conocimiento. Sugiere la creación de un Comité de transición. Enumera un proceso genérico de actividades para la devolución del servicio si fuera necesario. Enumera herramientas para la transición, sin detallar un plan progresivo de la plataforma SIEM.
Mejora de los Acuerdos de Nivel de Servicio	2,5	1,20	Proponen tres indicadores adicionales, dos de ellos relativos a disponibilidad.
Total Valoración	50	27,89	

2.3 Oferta de SOTHIS SERVICIOS TECNOLÓGICOS, SLU.

Criterios técnicos sometidos a juicio de valor	Valor máx.	Valor SOTHIS	Comentarios a oferta de SOTHIS
Solución Técnica y Metodología	15	11,26	
Servicios de la Oficina Técnica de Seguridad (OTS)	7,5	5,63	Presenta un modelo de análisis y adecuación al ENS y planes de mejora, aportando diseño de herramienta PowerBI para tenant de RTVE para seguimiento de vulnerabilidades y cumplimiento del Marco de controles ENS configurado a medida de RTVE. Su propuesta se basa en el Marco ENS requerido a RTVE. Propone que los controles ENS se mantengan reflejados en una herramienta y tenant propios de RTVE. Respecto a soporte a ciberincidentes, se presenta un modelo notable de gestión de alertas y medios, apoyada por un servicio de OTS con un diseño orientado a RTVE, con gestión de la herramienta Service Desk+ con las áreas técnicas de RTVE. Se propone un modelo de formación y concienciación (píldoras, formación intranet, ataques éticos…). Propone un modelo de bastionado y control, así como de gestión de vulnerabilidades, utilizando la herramienta nessus. Propone seguimiento de resultados en PowerBI configurado a medida de RTVE, integrado con el servicio del SOC. Respecto a gestión de la capacidad y demanda, presenta un modelo apoyado en múltiples informes periódicos y herramienta SIGO, de RTVE, así como formularios Excel para seguimiento. Propone un plan de Gestión del Servicio describiendo todos los procesos operativos, orientados a RTVE.

Servicios Especializados	7,5	5,63	Propone seguimiento cíclico de eventos con soporte de herramientas de vigilancia e interlocución con las áreas técnicas implicadas de RTVE. Aporta capacidad de soporte a eventos orientados a RTVE. Propone gestión de vulnerabilidades y amenazas enfocado a activos y perimetral transversal en RTVE. Ofrece soporte al uso de herramientas concretas del CCN o privadas, así como estudios comparativos concretos orientados a RTVE. Propone modelo de integraciones con el SOC, adaptado a RTVE. Refiere la guía CCNSTIC-205 como modelo a seguir. Presenta un detallado modelo de Framework de seguridad frente a dominios operacionales y técnicos. Propone modelos de soporte adaptados al Responsable de Ciberseguridad de RTVE para informes tales como los precisos para el Comité de Ciberseguridad, Plan de Acción anual, Comités de Dirección, etc. Asume sin más lo requerido en pliego sobre metodología y herramientas de apoyo. Presenta un modelo apoyado en una metodología de gestión de las solicitudes adaptado a RTVE y soporte con herramientas como SIGO, Excel para seguimiento, etc. Propone un plan de Gestión del Servicio describiendo todos los procesos operativos, orientados a RTVE.
Equipo profesional	15	9,98	
Titulaciones	3,75	2,40	Todos los miembros del equipo cumplen la titulación requerida pero solo algunos aportan titulaciones adicionales de valor para el servicio.
Certificaciones adicionales de utilidad para el servicio	3,75	2,47	Solo algunos miembros presentan certificaciones adicionales a lo solicitado.
Formación tecnológica aplicable al servicio	3,75	1,96	Solo algunos miembros presentan alguna formación adicional de valor para el servicio.

Experiencia adicional aplicable al servicio	3,75	3,15	Solo algunos miembros cumplen con experiencia adicional aplicable al servicio.
Capacidades de SOC	15	10,80	
Metodología y procesos internos	3	2,25	Se describe en detalle servicios internos como Oficina de Peticiones (ServiceDesk+), servicio de alerta temprana, servicio de emisión proactiva de indicadores de compromiso, servicio gestión de vulnerabilidades, servicio de monitorización y gestión de incidentes, servicio modelado de amenazas, servicio de respuesta y análisis forense, servicio de mejora del servicio, percibiendo excelente orientación a las necesidades de RTVE. Presenta un modelo de procesos internos y gestión de la demanda apoyado en una metodología de gestión de las solicitudes orientado a RTVE y soporte con herramientas como SIGO, Excel para seguimiento, informes mensuales del SOC, orientados a RTVE. Propone un plan de Gestión del Servicio describiendo todos los procesos operativos de gestión, orientados a RTVE.

Medios tecnológicos y herramientas	3	2,85	Propone la herramienta estándar ServiceDesk+ para gestión de alertas con áreas técnicas, Nessus para gestión de vulnerabilidades, SIEM IBM Qradar, etc. Se enumeran y describen los elementos de monitorización NIDS, HIDS, etc. ESET threat intelligence, Cisco Tales, MISP (comunicación de alertas con CCN) y enumera de forma genérica fuentes de inteligencia. Propone añadir UBA (comportamiento anómalo de usuarios). Indica IBM Soar como plataforma de orquestación de operaciones de seguridad, adaptado a RTVE.
Flexibilidad para picos de trabajo no previstos	3	2,25	Pone a disposición servicios de un Helpdesk propio para atender solicitudes por encima de la demanda, sin percibir total orientación a las necesidades de RTVE.
Coordinación entre el equipo de personal in situ y remoto	3	1,20	Expone de forma genérica actividades de periodicidad diaria", inicio y fin de semana indicando que se basan en metodologías agile (gestión de proyectos) sin percibir propuestas adicionales de valor para RTVE.
Homologaciones del SOC	3	2,25	Indica ENS Alto en servicios Operativos del SOC, sin apreciar homologaciones adicionales de valor para el servicio.
Aspectos generales del servicio	5	3,38	

Plan de transición y recursos disponibles	2,5	1,00	Contempla fase de transición de entrada en el Servicio. Presenta un modelo y metodología general de gestión del despliegue y seguimiento del servicio, según requiere el pliego, sin percibir total orientación a la situación en RTVE. Aporta un plan genérico de salida.
Mejora de los Acuerdos de Nivel de Servicio	2,5	2,38	Presenta mejora en los ANS solicitados en el pliego , tanto en tiempo de respuesta como calidad, y adicionalmente se propone una notable ampliación en el número de ANS, si bien se podría mejorar algún objetivo o métrica presentada.
Total Valoración	50	35,42	

3 Cuadro-resumen de valoración de ofertas.

La siguiente tabla refleja la puntuación asignada a cada una de las empresas en los apartados contemplados en el pliego.

Criterios técnicos sometidos a juicio de valor	Valor máx.	Valor SIA	Valor SOTHIS
Solución Técnica y Metodología	15	8,63	11,26
Servicios de la Oficina Técnica de Seguridad (OTS)	7,5	5,63	5,63
Servicios Especializados	7,5	3,00	5,63
Equipo profesional	15	8,76	9,98
Titulaciones	3,75	1,50	2,40
Certificaciones adicionales de utilidad para el servicio	3,75	2,22	2,47
Formación tecnológica aplicable al servicio	3,75	1,48	1,96
Experiencia adicional aplicable al servicio	3,75	3,56	3,15
Capacidades de SOC	15	8,30	10,80
Metodología y procesos internos	3	1,40	2,25
Medios tecnológicos y herramientas	3	2,25	2,85
Flexibilidad para picos de trabajo no previstos	3	1,20	2,25
Coordinación entre el equipo de personal in situ y remoto	3	1,20	1,20
Homologaciones del SOC	3	2,25	2,25
Aspectos generales del servicio	5	2,20	3,38
Plan de transición y recursos disponibles	2,5	1,00	1,00
Mejora de los Acuerdos de Nivel de Servicio	2,5	1,20	2,38
Total Valoración	50	27,89	35,42

4 Conclusiones sobre las ofertas presentadas

Las ofertas presentadas y no excluidas cumplen con los requisitos técnicos exigidos en el pliego de especificaciones técnicas, por lo que la adjudicación ha de realizarse a partir de los criterios técnicos reflejados en este informe y los económicos que a tal efecto determine la Dirección de Compras de CRTVE.