

## **MEMORIA JUSTIFICATIVA**

### **S-03286-2026 - Servicio Integral de Ciberseguridad SIC27**

#### **JUSTIFICACIÓN DE LA NECESIDAD:**

RTVE desarrolla una parte esencial de su actividad mediante procesos y plataformas digitales, tanto de tecnologías de la información como de tecnologías operacionales, que dan soporte a funciones corporativas, productivas y de explotación audiovisual. La continuidad, integridad, disponibilidad y confidencialidad de dichos sistemas resulta imprescindible para la prestación del servicio público encomendado a RTVE.

El contrato en vigor para este servicio (*expediente S-06041-2022 - Servicio Integral de Ciberseguridad SIC23*) finalizará el 30 de junio de 2027.

La necesidad a cubrir mediante este expediente consiste en continuar un SERVICIO integral de ciberseguridad, actualizado a la realidad operativa que dé soporte de forma coordinada a las tres áreas técnicas de RTVE así como al resto de la Corporación según la necesidad de análisis y gestión de incidentes mediante CSIRT. El SERVICIO debe articularse mediante un Centro de Operaciones de Seguridad (SOC) y una Oficina Técnica de Seguridad (OTS) que, bajo coordinación y control de la Unidad de Ciberseguridad de RTVE (Dir. Seguridad Corporativa), trabajen sobre una misma visión de riesgos, alertas, integraciones, procedimientos y seguimiento. La dimensión de personal a asignar al SERVICIO es decisión del licitador para asegurar la prestación de Servicio requerido.

En el ámbito SOC, el servicio debe mantener la monitorización, análisis y escalado de eventos y alertas de seguridad generadas en las áreas indicadas, apoyándose en las sondas y recolectores desplegados y en las integraciones actualmente existentes con herramientas y servicios como Wazuh, Zeek, Microsoft 365, Microsoft Defender, VMware ESXi, firewalls, soluciones de identidad, protección del correo, MDM, antivirus y otras fuentes de registro y telemetría. Todo ello exige capacidad de correlación, análisis continuo y respuesta coordinada.

En el ámbito OTS, el servicio debe ejecutar tanto tareas bajo demanda como tareas cíclicas de apoyo a la Unidad de Ciberseguridad de RTVE, entre otras: análisis ligero de software, pre-análisis de correos sospechosos, restablecimiento de credenciales comprometidas, revisión y reasignación de tickets en Service Desk +, elaboración de contenidos de formación, campañas de concienciación y simulación de smishing, phishing, vishing, Qrishing, etc, extracción y revisión de indicadores de actividad sospechosa, análisis de vulnerabilidades, revisiones de bastionado, controles sobre firewalls, administradores, accesos a O365 y otros controles periódicos de seguridad.

Asimismo, la prestación requiere, de forma puntual y estrictamente vinculada al diagnóstico y tratamiento de alertas e incidentes según su criticidad, acceso a información y trazas que pueden contener datos personales, tales como identificadores de usuario, direcciones IP, registros de acceso, metadatos de correo, información de cuentas de Microsoft 365 o tickets de gestión. Esta circunstancia refuerza la necesidad de contratar un servicio especializado, maduro y sujeto a garantías técnicas y organizativas adecuadas.

En consecuencia, procede la contratación de SIC27 como servicio integral y continuado de ciberseguridad para RTVE.

#### **INFORME DE INSUFICIENCIA DE MEDIOS**

Para la correcta ejecución de los trabajos se requieren recursos humanos altamente especializados y certificados en materias como operación SOC 24x7, gestión y correlación de eventos, respuesta a incidentes, análisis de amenazas, gestión de vulnerabilidades, bastionado, análisis de logs, revisión de configuraciones de seguridad,

concienciación y cumplimiento normativo. RTVE no dispone de medios propios suficientes con ese grado de especialización y disponibilidad continuada.

Del mismo modo, RTVE no dispone de un Centro de Operaciones de Seguridad propio, con la infraestructura, herramientas, procedimientos y capacidad operativa necesarios para prestar de forma integrada el servicio sobre las áreas técnicas citadas, así como al resto de la Corporación según la necesidad de análisis y gestión de incidentes, ni para asumir la evolución y mantenimiento de las integraciones y controles actualmente implantados.

Por todo ello, resulta necesaria la contratación de un proveedor especializado que aporte los medios humanos, técnicos y organizativos necesarios para la prestación del servicio en las condiciones de calidad, continuidad, trazabilidad y seguridad requeridas.

### **LOTES DE LA CONTRATACIÓN**

El expediente se plantea en un único lote.

El objeto del contrato no resulta divisible en lotes. SIC27 configura un servicio integral en el que el SOC y la OTS comparten información, procedimientos, herramientas, entregables e interlocución operativa sobre las áreas técnicas citadas. La eventual división por lotes dificultaría la correcta correlación de eventos, el tratamiento homogéneo de alertas, la coordinación de las actuaciones de análisis, contención y remediación, así como el seguimiento continuo de tareas recurrentes y bajo demanda.

Asimismo, la prestación requiere una gestión unitaria de herramientas y servicios de seguridad, de sus integraciones y de la documentación operativa asociada. La alta complejidad técnica del servicio hace aconsejable que dichas funciones se desplieguen y administren por un único adjudicatario, garantizando uniformidad metodológica y responsabilidad extremo a extremo.

La separación por lotes incrementaría los tiempos de respuesta ante incidentes de ciberseguridad complejos, multiplicaría los puntos de coordinación, aumentaría el coste de gestión y podría comprometer el cumplimiento de los acuerdos de nivel de servicio. Además, la participación de distintos adjudicatarios pondría en riesgo la homogeneidad de criterios técnicos, la trazabilidad de las actuaciones y la continuidad operativa del servicio, especialmente en actuaciones que requieren escalado inmediato entre OTS, SOC y CSIRT. Contar con diferentes proveedores aumentaría el coste y reduciría la eficiencia global del servicio.

La entidad contratante podrá no dividir en lotes el objeto del contrato cuando existan motivos válidos. En este caso, la realización independiente de las diversas tareas comprendidas en el objeto del contrato dificultaría su correcta ejecución, tanto desde el punto de vista técnico como por la necesidad de coordinar de forma inmediata y permanente la ejecución de trabajos interdependientes.

En conclusión, procede a los efectos del art. 99 de la Ley 9/2017 de Contratos del Sector Público, la no división en lotes del contrato para esta prestación.

### **JUSTIFICACIÓN DEL PROCEDIMIENTO**

Se propone el trámite de este expediente por un procedimiento abierto, sujeto a regulación armonizada, ya que no concurren los requisitos previstos en la LCSP para acudir a un procedimiento distinto y resulta el cauce más adecuado para una contratación de esta naturaleza, importe, duración y criticidad.

El procedimiento abierto es garantía de transparencia, publicidad e igualdad de trato entre los licitadores y favorece la máxima concurrencia en un mercado especializado pero competitivo, permitiendo seleccionar la oferta con mejor relación calidad-precio.

## JUSTIFICACIÓN DE LOS CRITERIOS DE SOLVENCIA

Se justifican a continuación los criterios de solvencia que deberán recogerse en el PCAP, por su relación directa con el objeto del contrato y por resultar proporcionales a la complejidad técnica, criticidad y alcance del servicio.

### **Solvencia económica:**

1. Tener un volumen anual de negocios referido a alguno de los tres últimos ejercicios disponibles igual o superior a 1.226.547,54 €, que equivale a una vez y media el importe anual del contrato. Se considera que un volumen anual de negocios, en alguno de los tres últimos ejercicios, de al menos 1,5 veces el importe anual del contrato es suficiente para garantizar que el licitador tiene capacidad económica para realizar el servicio y no es un volumen de negocio excesivo, de forma que no se restrinja la concurrencia.

### **Solvencia técnica:**

2. Contar al menos con tres (3) referencias de trabajos similares al objeto del contrato, realizados en los últimos 3 años cuyo importe acumulado sea igual o superior al 70 % del importe anual del contrato (572.388,85 euros).

Se consideran trabajos similares aquellos servicios de SOC, OTS y/o CSIRT similares a los definidos en el objeto de este contrato. Al menos una de las referencias deberá corresponder a un servicio continuado con una duración mínima de 18 meses y las otras dos con una duración mínima de 3 meses. Todas las referencias aportadas deberán haberse prestado con el mismo SIEM que el ofertado.

Las tres (3) referencias de prestaciones similares son necesarias para acreditar que el licitador dispone de capacidad, experiencia y madurez operativa suficientes para ejecutar un servicio altamente especializado, multidisciplinar y crítico, que integra monitorización SOC, gestión de alertas, soporte técnico de ciberseguridad y tareas operativas recurrentes y bajo demanda. El umbral del 70 % del importe anual del contrato es proporcionado, asumible para el sector y adecuado para demostrar experiencia contrastada en el objeto del contrato.

La duración de 18 meses de una de las referencias es una experiencia que razonablemente excede una implantación inicial o un proyecto de corta duración. Comprende al menos un ciclo anual completo de operación más un periodo adicional en el que hayan podido repetirse y mejorarse los procesos. Es razonable esperar que durante ese periodo el proveedor haya tenido que enfrentarse a variaciones de carga, rotaciones del equipo, cambios tecnológicos, incorporación de nuevas amenazas y diferentes tipos de incidentes. A estos efectos, se considera proporcionada una experiencia mínima de dieciocho meses en servicios de naturaleza y alcance similares por suponer haber atravesado razonablemente más de un ciclo de evolución de la plataforma y del servicio —mantenimiento, cambios de versiones, incorporación de nuevas fuentes y modificación de reglas—, lo que aporta evidencia adicional sobre la capacidad del proveedor para mantenerla en condiciones reales de producción

La exigencia de experiencia mínima operando en servicios similares el SIEM ofertado (pieza crítica dentro del modelo de prestación del SOC), se debe a que constituye un elemento fundamental para la ingesta y correlación de eventos, generación y gestión de alertas e investigación de incidentes. Se considera necesario que el adjudicatario disponga de experiencia suficientemente consolidada en la explotación en producción de la solución propuesta, evitando que la fase inicial del contrato constituya un periodo de aprendizaje de la propia tecnología ofertada y reduciendo con ello el riesgo sobre los niveles de detección y respuesta requeridos.

3. Disponer de documentos acreditativos de que el licitador se encuentra en un proceso de mejora continua para aumentar la satisfacción del cliente. Se podrá acreditar mediante la presentación de la

certificación de calidad ISO 9001 o cualquier otro elemento de prueba alternativo, que indicará en el Anexo II Declaración responsable.

4. Disponer de documentos acreditativos de que el licitador domina la gestión de los riesgos de seguridad de la información, así como a identificar y evaluar los posibles riesgos sobre la misma. Se podrá acreditar presentando la certificación de seguridad de la información ISO 27001 o cualquier otro elemento de prueba alternativo, que indicará en el Anexo II Declaración responsable.

Se considera imprescindible exigir dichas certificaciones, acreditaciones y pertenencias porque están directamente relacionadas con la calidad, fiabilidad y garantías de seguridad con las que debe prestarse el servicio, así como con la capacidad real del adjudicatario para operar un SOC y OTS maduros, gestionar incidentes y tratar información sensible en un entorno crítico. El cumplimiento de estos requisitos garantiza un umbral mínimo de calidad, resiliencia y especialización técnica, reduce riesgos de ejecución y aporta a RTVE mayores garantías en relación con la operación continuada del servicio, la respuesta ante incidentes y la protección de la información tratada.

## JUSTIFICACIÓN DE LOS CRITERIOS DE VALORACIÓN

La aplicación de los criterios de valoración definidos en la cláusula 11<sup>a</sup> del PCAP, permitirá que la oferta que resulte adjudicada sea la más adecuada, para cubrir las necesidades de RTVE.

- Criterios de valoración técnicos sujetos a juicio de valor: 28 puntos
- Criterios de valoración técnicos – automáticos: 23 puntos
- Criterios de valoración automática – precio: 49 puntos

### 1) Criterios de valoración técnicos sujetos a juicio de valor

#### - **Solución técnica y metodología. (máximo 14 puntos)**

##### • **Oficina Técnica de Seguridad (máximo 3 puntos):**

Garantiza una capacidad especializada para gobernar, coordinar y mejorar de forma continua la seguridad, asegurando seguimiento técnico, control del servicio y adecuada coordinación entre los distintos ámbitos operativos.

##### • **Capacidad de integración por el fabricante del SIEM (máximo 8 puntos):**

Reduce incompatibilidades, desarrollos ad hoc y tiempos de integración, favoreciendo una interoperabilidad estable con las herramientas del CCN y una mayor trazabilidad, soporte y mantenibilidad de las conexiones implantadas.

##### • **Capacidad de integración con ELSA (máximo 3 puntos):**

Permite integrar y automatizar el ciclo de gestión de vulnerabilidades, consolidando distintas fuentes y reduciendo tareas manuales, tiempos de tratamiento, errores operativos y pérdidas de trazabilidad en su seguimiento.

#### - **Capacidades de SOC - Experiencia del equipo de trabajo (máximo 7 puntos):**

Reduce la curva de aprendizaje y el riesgo operativo al acreditar experiencia real en el SIEM ofertado, favoreciendo una explotación más eficaz desde el inicio y una resolución solvente de situaciones complejas.

- **Herramientas y capacidades (máximo 4 puntos)**

• **Motor de correlación (máximo 2 puntos):**

Favorece una correlación rápida, determinista y trazable ante grandes volúmenes de eventos y reglas complejas, mejorando la capacidad de detección y la explicación técnica de las relaciones identificadas.

• **Integración nativa (máximo 1 punto):**

Reduce el esfuerzo, coste y riesgo de integraciones específicas, facilitando el intercambio ágil de incidentes e inteligencia de amenazas y acelerando los procesos de investigación, enriquecimiento y respuesta coordinada.

• **CMDB (máximo 1 punto):**

Aporta contexto de activos, criticidad y riesgos para priorizar alertas e incidentes con mayor precisión, automatizando su relación con información de riesgo y mejorando el análisis de impacto y la toma de decisiones.

- **Aspectos generales del servicio (máximo 3 puntos):**

• **Plan de transición (máximo 0,5 puntos):**

Minimiza pérdidas de conocimiento, interrupciones y degradaciones durante la entrada o salida del adjudicatario, asegurando una transferencia ordenada, verificable y progresiva de responsabilidades, información y capacidades operativas.

• **Mejora de los Acuerdos de Nivel de Servicio (máximo 1,5 puntos):**

Incentiva niveles de servicio superiores en actividades críticas de seguridad, reduciendo ventanas de exposición y mejorando la rapidez de actuación, disponibilidad y capacidad de recuperación ante eventos relevantes. Permite valorar aportaciones adicionales, concretas y verificables que incrementen la calidad, eficacia o resiliencia del servicio, siempre que supongan una mejora efectiva respecto de las condiciones mínimas exigidas.

• **Modelo CSIRT (máximo 1 punto):**

Garantiza un modelo de respuesta coordinado y estructurado para incidentes relevantes, definiendo activación, escalado, herramientas y responsabilidades y reduciendo solapamientos, demoras y riesgos de descoordinación entre CSIRT, SOC y OTS.

2) **Criterios de valoración técnicos automáticos**

- **Capacidad de que SOC y CSIRT sean ejecutados directamente por el adjudicatario (2 puntos)**

Se consideran tareas críticas aquellas correspondientes a la operación de los servicios SOC y CSIRT

Estas actividades constituyen un núcleo funcional único e interdependiente dentro del servicio integral de ciberseguridad. Su ejecución requiere mecanismos comunes de actuación y escalado y una trazabilidad extrema a extremo desde la detección de una amenaza hasta su análisis, contención, resolución y posterior incorporación de las lecciones aprendidas. La intervención de organizaciones adicionales en dicho núcleo introduciría interfaces operativas adicionales en procesos sometidos a exigentes tiempos de respuesta, incrementando el riesgo de pérdida de información, retrasos en el escalado o divergencias en los criterios de actuación. Asimismo, la ejecución de dichas funciones requiere el acceso continuado a información

especialmente sensible sobre la arquitectura de los sistemas, configuraciones de seguridad, vulnerabilidades, registros de actividad, reglas y mecanismos de detección e información relativa a incidentes de seguridad, pudiendo comportar además accesos privilegiados a determinados sistemas.

Por ello, evaluar positivamente la ejecución de estas tareas por parte del adjudicatario, sin subcontratación, reduce el número de entidades que acceden a dicha información y sistemas y disminuye el riesgo asociado a la cadena de suministro, facilitando asimismo el mantenimiento de una cadena de custodia, control de accesos y trazabilidad homogéneas.

- **Capacidad de proporcionar certificados conforme a la Guía CCN-STIC 896 para los servicios definidos (máximo 4 puntos):**

Aportan evidencia objetiva y verificable de capacidad y madurez en servicios de ciberseguridad alineados con la Guía CCN-STIC 896, reforzando la confianza en procesos, organización y capacidades del proveedor. Acreditan capacidad para gobernar, planificar y coordinar de forma estructurada los procesos de seguridad, favoreciendo una gestión consistente del servicio, sus riesgos, prioridades, recursos y mecanismos de seguimiento. Acreditan capacidad para anticipar amenazas y reducir su probabilidad de materialización mediante medidas preventivas estructuradas, contribuyendo a disminuir la superficie de exposición antes de que se produzcan incidentes. Acreditan capacidad para implantar y operar medidas de protección que limiten la exposición y el impacto de amenazas, reforzando la defensa de activos, servicios e información frente a escenarios de riesgo relevantes. Acreditan capacidad para identificar tempranamente eventos e indicios de compromiso mediante procesos de detección maduros, reduciendo el tiempo de permanencia de amenazas y facilitando una actuación más rápida y fundamentada. Acreditan capacidad para contener, gestionar y coordinar incidentes de forma organizada y eficaz, reduciendo su impacto, favoreciendo la recuperación y asegurando trazabilidad y consistencia durante las actuaciones de respuesta.

- **Capacidades de SOC - Capacidad de gestión de alertas (máximo 7 puntos):**

Justificación técnica: Reduce los tiempos de detección, análisis y propuesta de respuesta, permitiendo gestionar grandes volúmenes y picos de alertas de forma homogénea, trazable y eficiente sin degradar la calidad del servicio.

- **Agente monitor propio para la extracción y transporte de logs de sistemas cedentes (1 punto)**

Permite disponer de soporte extremo a extremo sobre la captura y transporte de logs, facilitando evolución coordinada, compatibilidad con el SIEM, diagnóstico de incidencias y capacidades remotas de monitorización y respuesta.

- **Equipo de trabajo (máximo 9 puntos):**

Permite valorar de forma objetiva una especialización y actualización técnica superior al mínimo exigido, aumentando la capacidad del equipo para abordar tecnologías, amenazas y situaciones operativas de distinta complejidad. En concreto, la justificación para cada perfil es:

- **Consultor de ciberseguridad (máximo 4 puntos):**

Refuerza la capacidad de análisis, diseño y asesoramiento técnico del consultor, aportando conocimientos acreditados adicionales para definir soluciones, evaluar riesgos y orientar decisiones en tareas de mayor complejidad.

- **Especialista de ciberseguridad (máximo 4 puntos):**

Acredita mayor profundidad técnica del especialista para operar herramientas, investigar eventos y resolver amenazas e incidencias avanzadas, reduciendo dependencias externas y mejorando la calidad y rapidez de la respuesta técnica.

- **Soporte ciberseguridad (máximo 1 puntos):**

Mejora la solvencia técnica del nivel operativo encargado del soporte y monitorización recurrente, favoreciendo diagnósticos más precisos, escalados adecuados y una atención más eficaz de incidencias y tareas habituales del servicio.

### 3) Criterios de valoración automática – precio (máx. 49 puntos)

Se aplican criterios automáticos para valorar el precio, la fórmula aplicada permite calificar adecuadamente las ofertas económicas asignando una puntuación según el precio ofertado de manera proporcional a la oferta más ventajosa.

Se establecerá un umbral mínimo para los criterios sujetos a juicio de valor del 35 % (recogido en la cláusula 9ª del PCAP), cuya consecuencia será la exclusión de aquellas ofertas que no lo superen. Se trata de una prestación crítica para la actividad diaria de RTVE. Aplicar este filtro permitirá que la prestación se ejecute con un alto grado de profesionalidad y alta capacidad, disminuyendo riesgos y garantizando el correcto funcionamiento. Se considera que las oferta que no alcancen esta puntuación no garantizan la ejecución optima de las prestaciones incluidas en el contrato.

### EXISTENCIA DE PRESUPUESTO

El presupuesto del CECO CC01SS2350 UNIDAD DE CIBERSEGURIDAD está aprobado y contempla esta contratación. La cuenta de gasto es la 6234003, servicios de Gestión para áreas técnicas, y el material asociado es el 8200562, servicios de gestión de sistemas.

El valor estimado de la contratación asciende a 4.415.571,14 € IVA no incluido, resultado de un importe contractual de 3.270.793,44 € para un periodo de cuatro años más un año de prórroga (817.698,36 €) y de una eventual modificación del 10 %, por importe de 327.079,34 €.

El desglose del importe contractual previsto es el siguiente:

- Servicio variable (Oficina de Ciberseguridad OTS y perfiles especializados de apoyo): 573.317,40 € anuales y 2.293.269,60 € para el total del contrato.
- Servicio fijo (Servicio de Vigilancia SOC): 244.380,96 € anuales y 977.523,84 € para el total del contrato.

En relación al expediente anterior:

|                     | <b>COSTE ANUAL</b> | <b>VALOR ESTIMADO</b> |
|---------------------|--------------------|-----------------------|
| <b>S-03286-2026</b> | 817.698,36 €       | 4.415.571,14 €        |
| <b>S-06041-2022</b> | 672.358 €          | 2.958.375,20 €        |
| <b>INCREMENTO</b>   | 145.340,36 €       | 1.457.195,94 €        |

Comparativamente, el coste anual previsto supone un 21,61 % de incremento sobre el coste anual estimado y un 49,26% sobre el valor estimado. Se espera que este incremento permita afrontar las siguientes situaciones tanto inesperadas como previsibles:

- El expediente actual incluye un año de **prórroga, lo cual no se previó en el contrato anterior.**
- **Incremento de los costes (laborales, fabricación, etc.) esperado** similar al previsible 2023-2027 (próximo al 10%). Según el INE, los costes entre junio de 2023 hasta julio de 2026 incluido, es de 9,5%
- Aproximación a la **tarifa real anual del SOC** (para esta partida **se tuvo que consumir el 9,9% de ampliación de contrato** además de limitar el gasto de EPS en el SIEM)

En el contrato en curso se estimaron 9.082 h anuales para servicios variables, sin embargo, en los últimos 12 meses el consumo anual requerido para dar el Servicio ronda las 12.000h (30% de incremento)

El valor estimado se ha determinado diferenciando una componente fija de vigilancia SOC y una componente variable asociada a la OTS y a perfiles especializados de apoyo, en función del volumen de servicio requerido y de la criticidad de las funciones a prestar.