

S-02583-2026**Mantenimiento y suscripción de licencias antivirus****MEMORIA JUSTIFICATIVA****OBJETO**

El presente expediente tiene por objeto la renovación de las licencias de las soluciones de seguridad TrendAI (anteriormente Trend Micro) que protegen los puestos de trabajo y los servidores corporativos de RTVE, la suscripción de nuevas capacidades de seguridad sobre esa misma plataforma y el soporte Premium 24x7x365 del fabricante durante toda la vigencia del contrato.

Renovación de las licencias existentes:

- Apex One on-prem: 5.001 dispositivos.
- XDR for Endpoints and Servers: 5.502 dispositivos.
- Deep Security Network Security: 501 servidores.
- Deep Security Malware Prevention: 501 servidores.
- Premium Support 24x7x365.

Suscripción de nuevas capacidades:

- Cyber Risk Exposure Management (CREM): 5.502 dispositivos.
- XDR for Networks (NDR): 500 Mb/s de caudal analizado.
- Análisis Sandbox: 5.502 dispositivos.
- AI Scanner y AI Guard: 5.000 peticiones diarias cada uno.

El contrato incluye asimismo la implantación, configuración, integración, pruebas y paso a operación de las nuevas capacidades, la transferencia de conocimiento, la documentación, los informes mensuales de servicio y de consumo de créditos y un Customer Success Manager asignado a la cuenta de RTVE. Todos estos servicios quedan comprendidos en el Soporte Premium y carecen de precio autónomo.

No se renuevan las 3 licencias de Portable Security 3 Pro incluidas en el contrato anterior, por haber dejado de utilizarse.

La duración del contrato será de 3 años desde el 1 de enero de 2027, con posibilidad de prorrogarse por 2 anualidades adicionales.

JUSTIFICACIÓN DE LA NECESIDAD:

La Dirección de Sistemas e Innovación dispone de licencias de productos del fabricante TrendAI (anteriormente Trend Micro) para la protección de los puestos de trabajo y los servidores corporativos frente al software malicioso y a la explotación de vulnerabilidades. Las licencias actualmente en vigor vencen el 31 de diciembre de 2026.

La proliferación de ataques cada vez más sofisticados, que se aprovechan de las vulnerabilidades de los equipos informáticos, puede dar lugar a incidentes graves de ciberseguridad, tales como:

- Robo de información del puesto de trabajo.
- Robo de credenciales de acceso a los sistemas de los usuarios.
- Utilización remota de los ordenadores corporativos para fines delictivos o dañinos.
- Intrusión, a través de los puestos de trabajo, en los servidores corporativos, llegando a provocar su inutilización o el robo de información corporativa.
- Cifrado de la información corporativa mediante ransomware, con la consiguiente parada de la actividad.

Asimismo, se dispone del agente de detección y respuesta en el punto final (EDR/XDR), que permite detectar ataques avanzados y comportamientos sospechosos como el movimiento lateral, correlacionar lo que ocurre simultáneamente en distintos equipos para frenar la propagación de un ataque, y conservar las evidencias necesarias para la investigación posterior. Toda esta información es monitorizada las 24 horas del día por el Centro de Operaciones de Ciberseguridad (SOC) desplegado por la Subdirección de Ciberseguridad, lo que permite reaccionar con rapidez en el momento en que se produce un ataque.

De no renovarse estas licencias, los equipos quedarían sin protección frente a código dañino y sin capacidad de detección y respuesta, lo que podría tener consecuencias graves, incluida la posible paralización de los puestos de trabajo y servidores de la red corporativa de RTVE.

Esta necesidad viene avalada por las recomendaciones del Centro Criptológico Nacional y por el Esquema Nacional de Seguridad, aprobado por el Real Decreto 311/2022, de 3 de mayo, que exige a las entidades del sector público implantar medidas de protección frente a código dañino, de gestión continua de vulnerabilidades y de monitorización y registro de la actividad.

Además de la renovación, se considera necesario ampliar las capacidades actuales por los siguientes motivos:

- Gestión de la exposición al riesgo (CREM). La protección del puesto final no cubre la gestión de la exposición. Esta capacidad permite descubrir de forma continua la superficie de ataque, identificar las vulnerabilidades y priorizarlas en función de su explotabilidad y de la criticidad del activo, dando respuesta a la exigencia de gestión continua de vulnerabilidades del Esquema Nacional de Seguridad.
- Seguridad de aplicaciones de inteligencia artificial (AI Scanner y AI Guard). La incorporación de aplicaciones basadas en inteligencia artificial generativa introduce vectores de riesgo nuevos —inyección de instrucciones, fuga de información sensible a través de las conversaciones y generación de contenido no admisible— que los controles actualmente desplegados no cubren.
- Detección y respuesta en red (NDR). Los agentes desplegados no ofrecen visibilidad del tráfico entre servidores ni de los dispositivos no gestionados. Esta capacidad permite identificar movimientos laterales, comunicaciones con servidores de mando y control y exfiltraciones de información que no son observables desde el puesto de trabajo.

- Análisis en entorno aislado (Sandbox). Permite emitir un veredicto sobre ficheros desconocidos y amenazas de día cero que las firmas y la heurística no resuelven, e incorporar automáticamente los indicadores de compromiso obtenidos al resto de la plataforma para su bloqueo inmediato.

Por último, la contratación conjunta permite alinear en una única fecha de vencimiento licencias que hoy proceden de expedientes distintos, lo que simplifica la gestión y evita el riesgo de interrupciones de la protección por desfases entre renovaciones.

La justificación de la referencia a una marca determinada. Los pliegos identifican productos del fabricante TrendAI (Trend Micro Incorporated), conforme al artículo 126.6 de la LCSP, esta referencia resulta justificada porque el objeto principal del contrato es la renovación de licencias ya desplegadas sobre una plataforma existente en RTVE, con agentes instalados en más de 5.000 puestos de trabajo y 501 servidores, integrada con la consola de gestión centralizada y con los procedimientos del Centro de Operaciones de Ciberseguridad. No es posible describir el objeto mediante especificaciones suficientemente precisas e inteligibles sin desvirtuarlo, ya que lo que se contrata es precisamente la continuidad de esas licencias y de su soporte.

La sustitución de la plataforma por la de otro fabricante exigiría la desinstalación y reinstalación de agentes en la totalidad del parque, la pérdida de la telemetría histórica y de las reglas de detección ajustadas a lo largo de los años, y un coste de migración desproporcionado respecto del objeto de este contrato. En todo caso, la licitación no queda restringida a un único operador económico: el suministro puede ser ofertado por cualquiera de los partners autorizados del fabricante, que concurren entre sí en régimen de competencia.

INFORME DE INSUFICIENCIA DE MEDIOS

RTVE no dispone de medios propios para la realización de esta prestación. Se trata de servicios que únicamente puede prestar el fabricante del software, desde sus laboratorios de desarrollo y soporte, directamente o a través de sus partners autorizados.

La suscripción y el soporte llevan asociados servicios que no son replicables internamente: la actualización permanente de los ficheros de firmas y de los motores de detección, la actualización de versiones del software, el acceso a la base de datos técnica del fabricante, el análisis de nuevas amenazas en sus laboratorios y el escalado a su ingeniería.

Las nuevas capacidades objeto del contrato (CREM, NDR, Sandbox, AI Scanner y AI Guard) se prestan en modalidad SaaS desde la plataforma del fabricante, por lo que su ejecución con medios propios resulta materialmente imposible.

La Dirección de Sistemas e Innovación no dispone de personal ni de infraestructura para asumir estas funciones, ni existe en RTVE ninguna otra unidad que preste servicios equivalentes o de similares características.

LOTES DE LA CONTRATACIÓN

El expediente se ha planteado en un único lote.

El objeto del contrato no resulta divisible: todas las prestaciones corresponden a licencias, créditos y soporte de una única plataforma tecnológica del mismo fabricante, integrada de forma nativa. El valor de la solución para RTVE reside precisamente en esa integración, ya que la correlación entre la protección del puesto de trabajo, la detección en red, el análisis en entorno aislado y la gestión de la exposición al riesgo se produce dentro de la propia plataforma.

A ello se añade que la mayor parte de las capacidades se licencia mediante una bolsa única de créditos (TrendAI Vision One Flex Credits) que se consume de forma conjunta y se reasigna entre capacidades según las necesidades. Su división en lotes obligaría a fraccionar artificialmente esa bolsa, impediría la reasignación de créditos y encarecería el conjunto.

El artículo 99.3 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, indica que el órgano de contratación podrá no dividir en lotes el objeto del contrato cuando existan motivos válidos, que deberán justificarse debidamente en el expediente. Entre esos motivos se cita, en su apartado b), el hecho de que la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultara su correcta ejecución desde el punto de vista técnico, o bien que el riesgo para la correcta ejecución proceda de la naturaleza del objeto, al implicar la necesidad de coordinar la ejecución de las diferentes prestaciones.

La ejecución independiente de estas prestaciones por adjudicatarios distintos dificultaría la correcta ejecución del contrato desde el punto de vista técnico e implicaría una necesidad de coordinación que pondría en riesgo la homogeneidad de criterios y la respuesta ante incidentes, en un ámbito — el de la ciberseguridad— en el que la fragmentación de responsabilidades constituye en sí misma un riesgo.

En conclusión, procede a los efectos del artículo 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 la tramitación de este expediente por procedimiento abierto sujeto a regulación armonizada, ya que no concurren los requisitos que establece la LCSP para tramitar esta contratación por un procedimiento distinto.

El procedimiento abierto es garantía de transparencia e igualdad de trato entre los licitadores y, además, garantiza la mayor concurrencia posible.

JUSTIFICACIÓN DE LOS CRITERIOS DE SOLVENCIA

Se justifica a continuación la elección de cada uno de los criterios de solvencia recogidos en la cláusula 8ª del PCAP.

Solvencia económica. Se exige un volumen anual de negocios, referido a alguno de los tres últimos ejercicios disponibles, igual o superior a 724.812,91 €, equivalente al 75 % del valor estimado del contrato.

Se considera que este umbral es proporcionado al objeto del contrato y no restrictivo de la concurrencia. Se trata de un contrato que puede alcanzar los cinco años de vigencia, cuya ejecución exige al adjudicatario capacidad para adquirir en el canal del fabricante volúmenes elevados de licencia y para sostener la prestación a lo largo del tiempo. El importe exigido resulta alcanzable por cualquier empresa del sector con capacidad de distribución acreditada y, además, se admite acreditarlo con cualquiera de los tres últimos ejercicios, lo que aporta flexibilidad a los licitadores.

Solvencia técnica. Se exige contar al menos con tres referencias de trabajos similares al objeto del contrato, ejecutados en los tres últimos años, cuyo importe acumulado sea igual o superior a 483.208,61 €, equivalente al 50 % del valor estimado del contrato. La exigencia de tres referencias persigue acreditar experiencia contrastada y no una ejecución aislada.

Sólo se considerarán trabajos similares los suministros de licencias de antivirus prestados a entidades con al menos 1.000 puestos de trabajo, con cobertura nacional y con una duración mínima de dos años. Esta definición responde a las características del parque de RTVE: un adjudicatario sin experiencia en despliegues de ese tamaño no podría garantizar la ejecución sin interrupciones del servicio, y la exigencia de dos años de duración acredita capacidad para sostener la prestación en el tiempo y no únicamente para realizar una entrega puntual.

Otros requisitos:

- Certificación ISO 9001 o medio de prueba equivalente. Acredita que el licitador se encuentra en un proceso de mejora continua orientado a la satisfacción del cliente, lo que resulta relevante en un contrato cuya calidad depende de la gestión del servicio a lo largo de un máximo de cinco años.
- Certificación ISO 14001 o equivalente. Acredita la adopción de medidas que fomentan la calidad del medio ambiente, en cuanto a protección ambiental y prevención de contaminación, y reducir impactos medioambientales negativos.
- Cumplimiento del Esquema Nacional de Seguridad en categoría MEDIA. Los sistemas y servicios empleados para la ejecución tratarán telemetría de seguridad procedente de la totalidad del parque de RTVE, información cuyo compromiso afectaría directamente a la seguridad corporativa. La exigencia se corresponde con la categoría de los sistemas afectados y es proporcionada al riesgo asumido.

Se considera imprescindible las certificaciones que se solicitan ya que éstas están directamente relacionadas con la calidad y garantías de seguridad con la que tienen que proporcionar las prestaciones objeto de este expediente.

El cumplimiento de estas normas de calidad garantiza la calidad y la buena gestión en la prestación y protección ambiental, con el fin de asegurar un buen resultado de la ejecución del contrato, minimizar los riesgos, y reducir los impactos medioambientales negativos.

Estas exigencias aseguran que el adjudicatario tenga la capacidad técnica, organizativa y de gestión necesarias para asumir la responsabilidad integral del servicio.

JUSTIFICACIÓN DE LOS CRITERIOS DE VALORACIÓN

La aplicación de los criterios de valoración definidos en la cláusula 11ª del PCAP permitirá que la oferta que resulte adjudicataria sea la más adecuada para cubrir las necesidades de RTVE. Se asignan 25 puntos a los criterios sujetos a juicio de valor y 75 puntos al precio.

El reparto de los 25 puntos responde al peso de cada aspecto en la ejecución del contrato:

- Acuerdos de nivel de servicio (10 puntos). Es el aspecto de mayor impacto, porque determina el tiempo de respuesta ante un incidente de seguridad, que constituye el factor crítico de este contrato.
- Procedimiento de apertura de incidencias y soporte (5 puntos). Condiciona la operativa diaria y la coordinación con el Centro de Operaciones de Ciberseguridad de RTVE.
- Equipo de trabajo y medios técnicos (5 puntos). Las certificaciones vigentes y la experiencia del equipo asignado son un indicador directo de la calidad previsible de la prestación, máxime cuando los servicios profesionales de implantación y la formación están incluidos en el precio del soporte.
- Entregables (5 puntos). La documentación, los informes de servicio y los planes de despliegue, transferencia de conocimiento y reversibilidad son los instrumentos que permiten a RTVE mantener el control efectivo del servicio.

Para evitar valoraciones basadas en declaraciones genéricas, la cláusula 11ª del PCAP establece una escala explícita de puntuación —propuesta muy adecuada, adecuada, suficiente o insuficiente— y advierte que no se otorgará puntuación a las propuestas que se limiten a reproducir los requisitos del pliego técnico sin aportar concreción sobre su ejecución.

El precio se valora con 75 puntos mediante una fórmula de proporcionalidad inversa respecto de la oferta más baja, que permite ordenar adecuadamente las ofertas económicas sin generar saltos desproporcionados de puntuación.

Umbral mínimo. Se establece un umbral mínimo de 10 puntos, equivalente al 40 % de los 25 puntos correspondientes a los criterios sujetos a juicio de valor. Su aplicación se justifica por tratarse de una prestación crítica para la actividad diaria de RTVE: una interrupción de la protección o una respuesta tardía ante un incidente de seguridad afectan a la totalidad de los puestos de trabajo y servidores corporativos. Se considera que una propuesta que no alcance el 40 % de la puntuación técnica no garantiza la ejecución del contrato en condiciones adecuadas, por lo que su admisión supondría un riesgo para el servicio.

EXISTENCIA DE PRESUPUESTO

El presupuesto está aprobado y contempla esta contratación con cargo a:

CONCEPTO	REFERENCIA
CECO	CC01SS2320 SISTEMAS Y EXPLOTACIÓN
Cuenta de gasto	6222002 Mantenimiento SW informático
Material	8200556 Mantenimiento SW informático

El valor estimado de la contratación asciende a 966.417,21 €, sin IVA, con el siguiente detalle:

CONCEPTO	IMPORTE SIN IVA
Contrato (3 anualidades, 2027-2029)	547.028,61 €
Prórrogas (2 anualidades, 2030-2031)	364.685,74 €
Modificación prevista (10 % del contrato)	54.702,86 €
VALOR ESTIMADO	966.417,21 €

El presupuesto base de licitación asciende a 547.028,61 € sin IVA —importe que comprende las tres anualidades del contrato, lo que supone 661.904,62 € con el 21 % de IVA. Los importes se han determinado a partir de precios actualizados solicitados al fabricante para el número de licencias y créditos requeridos, y se han trasladado a la cláusula 3ª del PCAP en forma de precios unitarios máximos.

Comparativa con el coste actual. El contrato vigente asciende a 155.941,89 € anuales. La comparación con el nuevo contrato es la siguiente:

CONCEPTO	ACTUAL (€/AÑO)	NUEVO (€/AÑO)	VARIACIÓN
Licencias y soporte objeto de renovación	151.122,39	131.871,75	-12,7 %
Portable Security 3 Pro (no se renueva)	4.819,50	0,00	-100 %
Nuevas capacidades (CREM, NDR, Sandbox, IA)	0,00	50.471,12	-
TOTAL	155.941,89	182.342,87	+16,9 %

El conjunto de prestaciones que se renuevan experimenta una reducción del 12,7 % respecto del contrato vigente, y ello pese a que el alcance protegido crece: el parque de servidores pasa de 422 a 501 licencias, un 18,7 % más, y la cobertura de XDR de 5.423 a 5.502 dispositivos.

El detalle por precios unitarios es el siguiente:

PRODUCTO	UNIDAD	2023-2026	2027-2029	VARIACIÓN
Apex One on-prem	dispositivo	4,55 €	4,50 €	-1,1 %
XDR for Endpoints and Servers	dispositivo	12,22 €	5,60 €	-54,2 %
Deep Security Network Security	servidor	16,79 €	21,55 €	+28,4 %
Deep Security Malware Prevention	servidor	7,20 €	9,50 €	+31,9 %
Premium Support	servicio	51.975,00 €	63.000,00 €	+21,2 %

La reducción se concentra en el módulo XDR, cuyo precio unitario disminuye un 54,2 % al pasar al modelo de créditos de la plataforma Vision One. Los módulos de Deep Security experimentan un incremento unitario derivado de la revisión de tarifas del fabricante, que queda ampliamente compensado por la reducción anterior. El incremento del Premium Support responde a la ampliación de su alcance: pasa a cubrir nueve productos en lugar de cinco e incorpora los servicios profesionales de implantación y la formación, que en el contrato anterior no estaban incluidos y habrían debido contratarse de forma independiente.

El incremento del importe total, del 16,9 %, corresponde íntegramente a las nuevas capacidades que se incorporan, que suponen 50.471,12 € anuales. Sin ellas, la renovación del contrato actual supondría un ahorro del 15,4 %.