



Expediente S-02583-2026

Mantenimiento y suscripción de licencias antivirus
TrendAI (2027)

Pliego de condiciones técnicas

Contenido

1	Introducción.....	3
2	Objeto y alcance	4
3	Situación actual	5
4	Requerimientos.....	6
4.1	Renovación de licencias	6
4.2	Adquisición nuevas licencias	7
4.2.1	CREM (Cyber Risk Exposure Management)	7
4.2.2	NDR (Network Detection and Response)	8
4.2.3	Análisis Sandbox.....	9
4.2.4	Herramientas Seguridad en Aplicaciones IA.....	11
4.2.5	Resumen de licencias.....	13
4.3	Soporte Premium 24x7 y Customer Success Manager.....	15
4.4	Integración con el Centro de Operaciones de Ciberseguridad.....	16
4.5	Reversibilidad y finalización del contrato	17
5	Transferencia de conocimiento.....	17
5.1	Sesiones técnicas y formación	17
5.2	Documentación obligatoria.....	17
6	Acuerdos de nivel de servicio	19
7	Incumplimientos graves del servicio.....	20
8	Estructura de las ofertas.....	21

1 Introducción

Radiotelevisión Española, en el marco de sus responsabilidades de protección de los sistemas de información corporativos, requiere mantener y reforzar las capacidades de ciberseguridad actualmente desplegadas para garantizar la continuidad del servicio, la protección frente a amenazas avanzadas y la evolución tecnológica de sus servicios de defensa, detección y respuesta.

RTVE dispone en la actualidad de distintas soluciones de seguridad del fabricante Trend Micro, en proceso de renombrado de marca comercial hacia TrendAI, orientadas a la protección de puestos de trabajo, servidores, entornos virtualizados y capacidades de detección y respuesta extendida.

A los efectos del presente pliego, y salvo indicación expresa en contrario, las referencias a «TrendAI» se entenderán realizadas al fabricante Trend Micro Incorporated y a sus productos, con independencia de la denominación comercial —Trend Micro o TrendAI— bajo la que figuren en las referencias de producto, SKU, certificaciones de partner, contratos de soporte o documentación técnica. Serán igualmente válidas a todos los efectos las acreditaciones y certificaciones expedidas bajo cualquiera de ambas denominaciones.

Dichas soluciones constituyen una parte esencial de la arquitectura de seguridad corporativa, por lo que resulta necesario asegurar su continuidad mediante la renovación de las licencias existentes, el mantenimiento del soporte especializado y la alineación de sus vencimientos en un marco contractual común.

Asimismo, la evolución del panorama de amenazas, el incremento de la superficie de exposición, la sofisticación de los ataques dirigidos y la aparición de nuevos vectores asociados al uso de inteligencia artificial hacen necesario ampliar las capacidades actuales con nuevas funcionalidades de gestión del riesgo cibernético, detección y respuesta en red, análisis avanzado en sandbox y protección específica de aplicaciones basadas en IA.

El presente Pliego de Condiciones Técnicas tiene por objeto definir los requisitos técnicos que deberán regir la contratación del mantenimiento y renovación de las licencias de seguridad existentes, así como la adquisición, implantación y soporte de nuevas capacidades integradas en la plataforma TrendAI Vision One.

La solución objeto del contrato deberá garantizar una gestión centralizada, integración nativa entre los distintos módulos, soporte premium 24x7, evolución tecnológica continua y capacidad de respuesta ante incidentes de seguridad, todo ello conforme a los niveles de servicio, condiciones técnicas y obligaciones establecidos en el presente pliego.

2 Objeto y alcance

El objeto del contrato es la prestación unificada de los siguientes suministros y servicios:

- Renovación de las licencias existentes de Apex One, XDR for Endpoints, Deep Security Network Security, Deep Security Malware Prevention y Premium Support.
- Adquisición de nuevas capacidades de Cyber Risk Exposure Management (CREM), Network Detection and Response (NDR), análisis Sandbox y seguridad de aplicaciones de inteligencia artificial mediante AI Scanner y AI Guard.
- Activación, diseño, implantación, configuración, integración, pruebas, documentación, transferencia de conocimiento y paso a operación de las nuevas capacidades, servicios que quedan incluidos en el Soporte Premium conforme al apartado 4.3.
- Soporte Premium 24x7 del fabricante, con Customer Success Manager (CSM) asignado a la cuenta de RTVE y servicios complementarios del adjudicatario.
- Seguimiento periódico, revisión de configuración, informes de servicio, control del consumo de licencias o créditos y asistencia durante toda la vigencia contractual.

Todas las licencias deberán quedar alineadas en fecha de vencimiento y no podrá producirse interrupción alguna en las protecciones existentes como consecuencia de la transición contractual.

3 Situación actual

En el marco de la Seguridad Informática, RTVE cuenta actualmente con los siguientes productos asociados al fabricante TrendAI, con vigencia hasta el 31 de diciembre de 2026:

Producto	Cantidad actual	Uso principal
Apex One on-prem	5.001 dispositivos	Protección de puestos de trabajo, VDI y equipos compatibles; gestión centralizada mediante Apex Central.
XDR for Endpoints and Servers	5.423 licencias	Telemetría, correlación, investigación y respuesta sobre endpoints y servidores.
Deep Security Network Security	422 servidores	IPS, protección de red y virtual patching para servidores.
Deep Security Malware Prevention	422 servidores	Protección antimalware de servidores físicos y virtuales.
Premium Support	1 servicio	Soporte prioritario 24x7x365 del fabricante.
Portable Security 3 Pro	3 licencias	No se renovarán en el presente contrato.

4 Requerimientos

4.1 Renovación de licencias

En este apartado se detalla la contratación del servicio de renovación de licencias de antivirus existentes utilizados en equipos clientes y servidores responsabilidad de la Dirección de Sistemas e Innovación, según el siguiente desglose:

Licenciamiento del contrato principal

Producto / referencia	SKU	Métrica y cantidad	Periodo
Trend Vision One Apex One on-prem, Government, 5.001-10.000, renovación	OS01142310	5.001 dispositivos	36 meses
Trend Vision One Flex Credits para XDR for Endpoints (EDR), renovación (5.502 dispositivos, 20 créditos por dispositivo y año)	V001227928	330.120 créditos ¹	36 meses
Deep Security Network Security per Server (VM), renovación	DX01002458	501 servidores	36 meses
Deep Security Malware Prevention per Server (VM), renovación	DX01007353	501 servidores	36 meses
Premium Support, extensión	PS01206966	1 servicio	36 meses

Licenciamiento de las prórrogas anuales de 12 meses

Producto / referencia	SKU	Métrica y cantidad	Periodo
Trend Vision One Apex One on-prem, Government, 5.001-10.000, renovación	OS01142310	5.001 dispositivos	12 meses
Trend Vision One Flex Credits para XDR for Endpoints (EDR), renovación (5.502 dispositivos, 20 créditos por dispositivo y año)	V001227928	110.040 créditos ¹	12 meses
Deep Security Network Security per Server (VM), renovación	DX01002458	501 servidores	12 meses
Deep Security Malware Prevention per Server (VM), renovación	DX01007353	501 servidores	12 meses
Premium Support, extensión	PS01206966	1 servicio	12 meses

¹ Equivalentes a 5.502 dispositivos a 20 créditos/dispositivo/año.

Se contempla una ampliación del parque de servidores durante la duración del nuevo contrato, pasando de 422 a 501 licencias asociadas a servidores respecto del contrato actual, lo que supone un incremento del 18,7 %.

De las 501 licencias de cada uno de los productos Deep Security Network Security y Deep Security Malware Prevention, 422 corresponden a renovación de licencias existentes y 79 a alta nueva. El licitador reflejará en su oferta económica la referencia y el precio unitario aplicables a cada uno de ambos conceptos cuando difieran.

Asimismo, la cobertura de XDR for Endpoints and Servers pasa de 5.423 a 5.502 licencias, en coherencia con el parque total de 5.001 puestos de trabajo y 501 servidores.

4.2 Adquisición nuevas licencias

Este apartado describe las nuevas licencias a adquirir por parte de RTVE, con el objetivo de incrementar la visibilidad y securizar nuevos vectores de infección.

4.2.1 CREM (Cyber Risk Exposure Management)

A continuación, se describen los objetivos primarios que debe cumplir la solución:

Descubrimiento continuo de superficie de ataque:

- Escaneo automático de activos expuestos a Internet (IPs, dominios, puertos, certificados)
- Identificación de shadow IT y activos no gestionados
- Inventario unificado correlacionado con AD/Azure AD

Identificación de vulnerabilidades críticas

- Escaneo con autenticación (profundidad total en sistemas)
- Escaneo sin autenticación (perspectiva del atacante)
- Cobertura: SO, aplicaciones, web, bases de datos, contenedores, cloud

Índices de riesgo y dashboards ejecutivos

- Puntuación global de riesgo cibernético (0-100)
- Puntuación por activo (criticidad + exposición + vulnerabilidades)

Integración nativa con el ecosistema TrendAI Vision One.

La solución deberá confirmar integración nativa demostrable con los siguientes componentes de la plataforma:

- TrendAI Vision One Endpoint Security (Apex One on-prem y agente cloud)
- TrendAI Vision One XDR for Endpoints (EDR)
- TrendAI Vision One XDR for Networks (NDR)

- TrendAI Apex Central
- TrendAI Deep Security (Network Security + Malware Prevention)
- Motor de automatización y playbooks de TrendAI Vision One
- Módulo de Inteligencia de Amenazas de TrendAI Vision One (Threat Intelligence / Suspicious Object Management)
- Módulo de Sandbox Analysis de Vision One

Priorización inteligente

- Basada en: CVSS + explotabilidad + exposición + criticidad de negocio

Requisitos técnicos obligatorios:

Requisito	Especificación
Despliegue	SaaS en cloud Vision One
Frecuencia de escaneo	Configurable: diario para críticos, semanal para resto
Tiempo de escaneo completo	< 6 horas para el inventario completo
Retención de datos	Mínimo 12 meses de histórico
Exportación de informes	PDF, CSV, JSON
Integración	Nativa con Vision One, API REST documentada

Se requiere licenciar el producto **CREM Core** para un total de 5502 dispositivos (incluyendo clientes y servidores).

Los escaneos autenticados se realizarán con cuentas de servicio proporcionadas y custodiadas por RTVE, con los privilegios mínimos necesarios. El licitador indicará los privilegios y protocolos de acceso requeridos para cada tipo de activo, así como el tratamiento y almacenamiento que la solución hace de dichas credenciales.

4.2.2 NDR (Network Detection and Response)

A continuación, se describen los objetivos primarios obligatorios:

Detección de amenazas en red

- Deep Packet Inspection (DPI) de tráfico norte-sur y este-oeste
- Detección mediante: firmas IPS + análisis comportamental + Machine Learning
- Identificación de: exploits, malware, C2, exfiltración, movimiento lateral

Despliegue

- Sondas virtuales: protección de activos internos virtualizados
- Sondas virtuales: protección de superficie expuesta a Internet (DMZ)

Integración con CREM

- Correlación de detecciones NDR con vulnerabilidades de CREM
- Priorización de alertas según criticidad de activos
- Visibilidad unificada en consola Vision One

Prevención de movimientos laterales

- Bloqueo automático de IPs, FQDNs, URLs maliciosas
- Integración con firewalls Fortinet
- Segmentación de red dinámica

Descubrimiento de activos

- Inventario dinámico de dispositivos en red
- Correlación con Azure AD, CMDB

Licenciamiento por 500Mb/s de throughput analizado.

Dimensionamiento y despliegue

El licenciamiento se dimensiona sobre un caudal analizado de 500 Mb/s. El licitador indicará expresamente en su oferta la equivalencia entre las unidades o créditos ofertados y el caudal analizado, y garantizará que la cantidad ofertada cubre dicho caudal.

El licitador propondrá en su oferta el número de sondas virtuales necesarias, su ubicación (red interna y DMZ) y los recursos de virtualización requeridos por cada una de ellas (vCPU, memoria, disco e interfaces de red), que serán aportados por RTVE sobre su infraestructura de virtualización corporativa.

RTVE facilitará el tráfico a analizar mediante puertos SPAN/mirroring o TAP virtual. El licitador especificará los métodos de captura soportados por cada sonda.

La integración con la plataforma de cortafuegos corporativa (Fortinet) para el bloqueo automático de direcciones IP, FQDN y URL se realizará mediante los mecanismos nativos de la solución. El licitador describirá el método de integración, los permisos requeridos y las versiones de FortiOS soportadas. RTVE facilitará el detalle del parque de cortafuegos a los licitadores que lo soliciten a través de la Plataforma de Licitación Electrónica.

4.2.3 Análisis Sandbox

La solución propuesta deberá incorporar un servicio de análisis en entorno aislado (sandbox) basado en tecnología cloud (Virtual Analyzer). Este servicio deberá estar integrado de forma nativa en la plataforma Vision One, del fabricante TrendAI, para garantizar continuidad operativa, integración nativa con agentes existentes, reducción de consolas y preservación de inversión ya desplegada.

La solución debe permitir el envío automático de objetos sospechosos detectados por los agentes de Endpoint Security desplegados en los puestos de trabajo y servidores del parque tecnológico

de RTVE. No se admitirán integraciones basadas en conectores de terceros, APIs intermediarias no nativas o consolas adicionales independientes para la gestión del sandbox.

Requisitos funcionales obligatorios. La solución de Sandbox deberá cumplir todos los requisitos funcionales descritos a continuación:

Envío automático de muestras desde Endpoint Security.

La solución deberá permitir configurar los agentes de TrendAI Vision One Endpoint Security (Standard Endpoint Protection / Apex One) para que envíen de forma automática y sin intervención del administrador los objetos sospechosos detectados al entorno sandbox cloud para su análisis. Los tipos de objetos enviados automáticamente deberán incluir, como mínimo:

- Programas desconocidos descargados a través de navegadores o canales de correo soportados.
- Ficheros detectados de forma heurística descargados a través de canales soportados.
- Programas de baja prevalencia con ejecución automática (autorun) desde almacenamiento extraíble.

La configuración del envío automático deberá realizarse mediante políticas gestionadas desde la consola centralizada de TrendAI Vision One, sin necesidad de acceder a consolas adicionales.

Análisis estático y dinámico avanzado.

El servicio sandbox deberá realizar tanto análisis estático (firmas, heurística, reputación de archivos y web) como análisis dinámico (simulación de comportamiento en entorno virtualizado aislado, detonación de la muestra) sobre los objetos enviados. El sandbox deberá ser capaz de detectar:

- Malware evasivo y amenazas desconocidas (zero-day).
- Ataques multi-fase: descargas desde URLs maliciosas, comunicaciones C&C (Command & Control).
- Exploits en documentos de ofimática y scripting.
- Archivos protegidos con contraseña.
- Scripts maliciosos (PowerShell, VBScript, JavaScript, etc.).
- Malware dirigido (targeted attacks).

Veredicto y niveles de riesgo.

Tras el análisis, el sistema deberá emitir un veredicto categorizado en niveles de riesgo: Alto, Medio, Bajo y Sin Riesgo. Cada veredicto deberá ir acompañado de un informe detallado que incluya, como mínimo:

- Naturaleza de la amenaza y comportamientos detectados.
- Artefactos identificados (modificaciones de registro, conexiones de red, ficheros creados/modificados).

- Mapeado de tácticas y técnicas según el framework MITRE ATT&CK™.
- Indicadores de Compromiso (IoC) generados: hashes SHA-1/SHA-256, dominios, URLs, IPs maliciosas.

La solución deberá permitir la descarga del paquete de investigación (investigation package) para los objetos con nivel de riesgo Alto, Medio y Bajo.

Integración con la inteligencia de la plataforma Vision One.

Los IoC identificados durante el proceso de análisis sandbox deberán ser incorporados automáticamente a la Lista de Objetos Sospechosos (Suspicious Object List) de TrendAI Vision One.

Dicha lista deberá ser distribuida automáticamente al resto de agentes y soluciones conectadas a la plataforma (Apex One, Deep Security, XDR for Networks, etc.) para activar acciones de bloqueo o cuarentena sobre las amenazas asociadas de forma inmediata.

Licenciamiento para un total de 5502 dispositivos.

4.2.4 Herramientas Seguridad en Aplicaciones IA

La proliferación de aplicaciones basadas en inteligencia artificial generativa introduce vectores de riesgo específicos —inyección de instrucciones (prompt injection), fuga de información sensible a través de las conversaciones y generación de contenido no admisible— que no quedan cubiertos por los controles de seguridad tradicionales. RTVE requiere incorporar capacidades de seguridad específicas para estas aplicaciones, tanto con carácter previo a su despliegue como en tiempo de ejecución.

4.2.4.1 AI Scanner

La solución deberá proporcionar una capacidad de análisis de seguridad de modelos y aplicaciones de inteligencia artificial con carácter previo a su puesta en producción, con las siguientes funcionalidades mínimas:

- Análisis de vulnerabilidades en LLM: deberá analizar el modelo y la aplicación en busca de debilidades estructurales, incluidas las recogidas en el OWASP Top 10 for LLM.
- Simulación de ataques adversarios: deberá ejecutar pruebas automatizadas de red teaming orientadas a detectar brechas de seguridad en el comportamiento del modelo.
- Detección de fuga de datos: deberá verificar si el modelo puede exponer información confidencial o datos de carácter personal.
- Cumplimiento normativo: deberá generar informes de riesgo documentados alineados con la normativa aplicable en materia de inteligencia artificial, incluido el Reglamento (UE) 2024/1689.

Se licenciará AI Scanner para un total de 5.000 peticiones diarias al servicio SaaS.

4.2.4.2 AI Guard

La solución deberá proporcionar una capacidad de inspección en tiempo real de las interacciones entre los usuarios y las aplicaciones de inteligencia artificial, aplicando políticas de seguridad, con las siguientes funcionalidades mínimas:

- Mitigación de prompt injection: deberá identificar y bloquear los intentos de alterar el comportamiento del modelo mediante instrucciones maliciosas.
- Filtrado de contenido y de salidas: deberá supervisar las respuestas del modelo para evitar la generación de contenido no admisible o la revelación de información sensible.
- Control de datos sensibles: deberá incorporar capacidades DLP que impidan el envío de información corporativa protegida a servicios de inteligencia artificial públicos o privados.
- Gobernanza y auditoría: deberá registrar de forma detallada las interacciones permitidas y bloqueadas, con fines de auditoría y análisis forense.

La inspección deberá poder integrarse mediante SDK o API y no introducirá una latencia adicional que degrade de forma apreciable el tiempo de respuesta de la aplicación protegida. El licitador indicará la latencia máxima introducida por el servicio.

Se licenciará AI Guard para un total de 5.000 peticiones diarias a la API del servicio.

A efectos de dimensionamiento, las 5.000 peticiones diarias indicadas para AI Scanner y las 5.000 peticiones diarias indicadas para AI Guard se entienden como media diaria calculada sobre un mes natural. El licitador indicará el tratamiento aplicable a los picos de demanda y el comportamiento del servicio en caso de superarse el umbral contratado (limitación, consumo adicional de créditos o denegación), sin que en ningún caso pueda producirse la interrupción de la aplicación protegida.

4.2.5 Resumen de licencias

Licenciamiento del contrato principal

Producto / referencia	SKU	Métrica y cantidad	Periodo
Cyber Risk Exposure Management Core (device). (5502 uds) (20 créditos por cliente al año), 12 months	V001239419	330.120 créditos	36 meses
XDR for networks (NDR) (1 uds) - 12500 Credits/unit, 12 months	V001239419	37.500 créditos	36 meses
AI Application Security (AI Guard y AI Scanner) (2 unidades) – SaaS - 9600 Credits/unit, 12 months	V001239419	57.600 créditos	36 meses
SandBox Analysis - Automatic Submission with Vision One Endpoint Security (5502 uds) - 7 Credits/unit, 12 months	V001239419	115.542 créditos	36 meses

Licenciamiento de las prórrogas anuales de 12 meses

Producto / referencia	SKU	Métrica y cantidad	Periodo
Cyber Risk Exposure Management Core (device). (5502 uds) (20 créditos por cliente al año), 12 months	V001239419	110.040 créditos	12 meses
XDR for networks (NDR) (1 uds) - 12500 Credits/unit, 12 months	V001239419	12.500 créditos	12 meses
AI Application Security (AI Guard y AI Scanner) (2 unidades) - SaaS - 9600 Credits/unit, 12 months	V001239419	19.200 créditos	12 meses
SandBox Analysis - Automatic Submission with Vision One Endpoint Security (5502 uds) - 7 Credits/unit, 12 months	V001239419	38.514 créditos	12 meses

Régimen de consumo de créditos

La totalidad de los créditos recogidos en las tablas anteriores se adquiere bajo el modelo TrendAI Vision One Flex Credits y constituye una bolsa única de créditos a disposición de RTVE.

El desglose por producto de las tablas anteriores tiene carácter indicativo y responde al dimensionamiento previsto en el momento de la licitación. RTVE podrá reasignar libremente los créditos entre las distintas capacidades comprendidas en el alcance del contrato, sin que ello constituya modificación del contrato ni genere coste adicional, siempre que no se supere el número total de créditos contratado.

Los créditos no consumidos al término de cada anualidad se acumularán a la anualidad siguiente dentro de la vigencia del contrato, incluidas sus prórrogas. El adjudicatario realizará ante el fabricante las gestiones necesarias para que dicho arrastre resulte efectivo.

El adjudicatario informará mensualmente del consumo de créditos por capacidad, del saldo disponible y de la proyección de agotamiento, y avisará a RTVE con una antelación mínima de dos meses cuando el consumo previsto pueda agotar la bolsa contratada.

El agotamiento de la bolsa de créditos no podrá suponer en ningún caso la interrupción de las protecciones en servicio.

4.3 Soporte Premium 24x7 y Customer Success Manager

La solución incluirá soporte Premium 24x7x365 del fabricante y un Customer Success Manager (CSM) asignado nominalmente a la cuenta de RTVE, con capacidad de atención en español.

El CSM será la figura de seguimiento y coordinación con el fabricante; no sustituirá a los canales técnicos de soporte ni a las obligaciones del adjudicatario.

Funciones mínimas del CSM

- Reunión de seguimiento, como mínimo, mensual.
- Revisión de estado de licencias, créditos, versiones, salud del servicio y adopción de capacidades.
- Coordinación de escalados con soporte, ingeniería y responsables del fabricante.
- Información sobre cambios de producto, fin de soporte, nuevas versiones y recomendaciones.
- Presentación de informes personalizados y plan de mejora.
- Participación en revisiones extraordinarias ante incidentes críticos o problemas recurrentes.

Servicios profesionales y formación incluidos

Los servicios profesionales necesarios para la puesta en servicio de las capacidades objeto del contrato —activación, diseño, configuración, integración con la plataforma y con los sistemas de RTVE, pruebas, elaboración de la documentación y paso a operación—, así como la transferencia de conocimiento descrita en el apartado 5, quedan incluidos en el Soporte Premium 24x7 y no serán objeto de facturación independiente.

En consecuencia, el precio ofertado para el Soporte Premium deberá cubrir la totalidad de dichos servicios, sin que el adjudicatario pueda repercutir a RTVE coste adicional alguno por jornadas de consultoría, desplazamientos, elaboración de entregables o impartición de las sesiones formativas.

El licitador detallará en su oferta el equipo asignado a estos servicios, los perfiles profesionales y la dedicación estimada para cada una de las capacidades a desplegar.

Plan de despliegue

El adjudicatario presentará, dentro de los 15 días naturales siguientes a la formalización del contrato, un plan de despliegue que recoja el alcance por capacidad, los hitos, las fechas, los recursos asignados y los interlocutores. El plan deberá ser aprobado por RTVE y contemplará, como mínimo, los siguientes hitos:

- Renovación de las licencias existentes activa y sin interrupción del servicio: 1 de enero de 2027.
- Alta y activación de las nuevas capacidades (CREM, NDR, Sandbox, AI Scanner y AI Guard): 15 de enero de 2027.
- Configuración, integración y pruebas de aceptación de cada nueva capacidad: 3 meses desde su activación.
- Entrega de la documentación As-Built y paso a operación: 15 días naturales desde la aceptación de cada capacidad.
- Ejecución completa del plan de transferencia de conocimiento: 6 meses desde la formalización del contrato.

4.4 Integración con el Centro de Operaciones de Ciberseguridad

RTVE dispone de un Centro de Operaciones de Ciberseguridad (SOC) que monitoriza de forma continua los eventos de seguridad. Todas las capacidades comprendidas en el alcance del contrato deberán poder integrarse con dicho SOC, permitiendo como mínimo:

- Envío de alertas, detecciones y eventos a sistemas externos de correlación (SIEM) mediante API REST documentada, syslog o conectores nativos, sin coste adicional de licenciamiento.
- Acceso de los analistas del SOC a la consola de Vision One con perfiles diferenciados y trazabilidad de las acciones realizadas.
- Exportación programada de la telemetría y de los indicadores de compromiso generados.

El licitador describirá en su oferta los mecanismos de integración disponibles, sus límites de volumen, frecuencia y retención, y si su uso consume créditos de la bolsa contratada.

4.5 Reversibilidad y finalización del contrato

A la finalización del contrato, por cumplimiento o por cualquier otra causa, el adjudicatario prestará sin coste adicional los servicios necesarios para garantizar la continuidad de la protección y la recuperación por RTVE de su información. Como mínimo:

- Entrega a RTVE, en formato abierto y documentado, de la telemetría histórica, los indicadores de compromiso, las políticas y las configuraciones existentes en la plataforma.
- Mantenimiento del acceso de consulta a la plataforma durante los 30 días naturales siguientes a la finalización, salvo imposibilidad técnica acreditada del fabricante.
- Elaboración de un informe de estado final del servicio y de las configuraciones desplegadas.
- Colaboración con el adjudicatario entrante o con el personal de RTVE durante el periodo de transición, con una dedicación mínima que el licitador cuantificará en su oferta.

5 Transferencia de conocimiento

5.1 Sesiones técnicas y formación

El licitador deberá proporcionar sesiones técnicas online dirigidas, orientadas a los perfiles técnicos y de gestión implicados en la administración, operación, detección, respuesta y gestión de riesgos de la solución.

El licitador deberá proporcionar acceso ilimitado al “*Education Portal de TrendAI*” durante la duración del contrato.

Las sesiones técnicas deberán contemplar, como mínimo, los siguientes contenidos, duración, audiencia y número de asistentes:

Curso	Duración	Asistentes
Vision One - Administración	2 días	10
APEX One	1 día	5
XDR - Detección y respuesta	3 días	10
CREM - Gestión de riesgos	2 días	8
NDR - Network Detection	2 días	8
AI Guard	1 día	12
AI Scanner	1 día	12

5.2 Documentación obligatoria

El licitador entregará, como mínimo, la siguiente documentación:

- Arquitectura implementada As-Built, incluyendo diagramas.
- Matriz de escalado, incluyendo árbol de decisión, contactos y SLAs.

Esta documentación se entregará dentro de los 15 días naturales siguientes a la finalización del despliegue de cada capacidad y se mantendrá actualizada durante toda la vigencia del contrato, incorporando los cambios que se produzcan en un plazo máximo de 15 días naturales.

El adjudicatario tiene obligación de documentar todas las actividades y tareas del servicio hasta el final del contrato, para ello se entregará a RTVE, como mínimo los informes mensuales, de seguimiento del servicio con fabricante y que incluirán:

- Incidencias y resolución de las mismas del período.
- Resultados de la revisión periódica de la configuración de los productos en RTVE, y propuesta de correcciones o mejoras.

Los informes mensuales se entregarán dentro de los diez primeros días hábiles del mes siguiente al periodo al que se refieran.

6 Acuerdos de nivel de servicio

El servicio incluirá soporte técnico (Premium Support) 24x7x365 prioritario, con los siguientes niveles de servicio:

Severidad	Definición	Respuesta inicial	Actualización
P1 - Crítico	Sistema caído, impacto producción	1 hora	Cada 4 horas
P2 - Alto	Funcionalidad degradada severa	4 horas	Cada 8 horas
P3 - Medio	Funcionalidad degradada moderada	8 horas laborables	Cada 24 horas
P4 - Bajo	Consulta general	24 horas laborables	Según progreso

Este soporte se presta con las siguientes características:

- **Canales:** teléfono directo, email, portal web
- **Idiomas:** español e inglés
- **Acceso:** ingenieros senior nivel 3, escalado directo a ingeniería del fabricante

Los tiempos comenzarán a computar desde la apertura por cualquiera de los canales habilitados.

El adjudicatario no podrá detener el cómputo salvo que dependa de información o actuación de RTVE claramente solicitada y documentada.

Para P1 y P2 se mantendrá seguimiento activo hasta la recuperación del servicio.

El escalado al fabricante no eximirá al adjudicatario de su responsabilidad de coordinación y comunicación.

Los informes mensuales incluirán el cumplimiento por severidad, promedios, máximos y causas de incumplimiento.

La empresa adjudicataria deberá disponer del certificado del fabricante TrendAI (Trend Micro Incorporated) como partner autorizado con nivel mínimo "Expert" para dar el soporte de sus producto.

Esta certificación podrá ser requerida por CRTVE, antes de la formalización del contrato, al tratarse de una condición esencial para la ejecución del contrato.

Disponibilidad de la plataforma

El adjudicatario garantizará una disponibilidad mensual mínima del 99,5 % de los servicios SaaS de la plataforma TrendAI Vision One incluidos en el alcance del contrato, medida sobre cada mes natural y excluyendo las ventanas de mantenimiento planificado comunicadas con una antelación mínima de cinco días hábiles. El informe mensual de servicio recogerá la disponibilidad efectiva alcanzada.

7 Incumplimientos graves del servicio

Dada la criticidad e importancia de los servicios objeto de este pliego por su impacto en procesos críticos para los usuarios de RTVE, el adjudicatario deberá asegurar el estricto cumplimiento del mismo sin deficiencias que puedan afectar al servicio prestado.

Se considerarán incumplimientos graves las siguientes situaciones:

- Retrasos superiores a 15 días naturales respecto de las fechas e hitos definidos en este pliego o de los plazos de ejecución de tareas específicas solicitadas por RTVE.
- No disponer el soporte de fabricante por la falta de actualización de los productos.
- Incumplimientos en el servicio que causen deficiencias en el funcionamiento por acciones u omisiones imputables a los servicios prestados por el adjudicatario. Entre ellas:
 - Indisponibilidad prolongada por más de 24 horas de la plataforma Vision One, Apex One o Deep Security.
 - Pérdida de información no recuperable.
 - Pérdidas de funcionalidad.
 - Pérdidas de rendimiento graves con afección al servicio provocadas por cualquier agente de la plataforma que se prolonguen durante más de 6 horas.
- Incumplimiento de los acuerdos de nivel de servicio durante 3 meses seguidos o 5 veces en un año.
- Incumplimiento de los valores mínimos / máximos de rendimiento solicitados en el pliego técnico.

8 Estructura de las ofertas

Las ofertas técnicas se estructurarán, como mínimo, conforme al siguiente índice:

1. Presentación.
2. Resumen ejecutivo.
3. Descripción de los productos a contratar.
4. Modelo de acuerdos de nivel de servicio.
5. Modelo de apertura de incidencias y peticiones.
6. Equipo de trabajo y medios técnicos asignados al contrato.
7. Entregables y plan de documentación.
8. Plan de despliegue e hitos.
9. Plan de transferencia de conocimiento.
10. Declaración de ubicación de los datos, subencargados y certificaciones de seguridad del servicio.
11. Plan de reversibilidad.

El licitador cumplimentará asimismo una matriz de cumplimiento en la que indique, para cada requisito del apartado 4, si la solución ofertada lo cumple y mediante qué componente o funcionalidad.