



TeleMadrid

SERVICIO GESTIONADO DE MANTENIMIENTO Y SOPORTE DE LA SOLUCIÓN CORPORATIVA DE ANTIVIRUS

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Dirección de Operaciones y Tecnología
Subdirección de Sistemas de Información

Enero 2026

Este documento es copia del original firmado. Se han ocultado datos personales en aplicación de normativa vigente.

ÍNDICE

1. OBJETO.....	3
2. ALCANCE.....	3
3. SERVICIO DE SOPORTE Y MANTENIMIENTO.....	4
4. NIVELES DE SERVICIO Y PENALIZACIONES.....	5
5. CONTENIDO DE LAS OFERTAS TÉCNICAS	7

Este documento es copia del original firmado. Se han ocultado datos personales en aplicación de la normativa vigente.

1. OBJETO

El objeto del presente pliego es establecer las condiciones técnicas que han de regir la contratación de la renovación, mantenimiento y soporte de licencias de antivirus “Kaspersky Advance” para puestos de trabajo y servidores, así como las herramientas necesarias para su administración, operación y gestión.

2. ALCANCE

RTVM dispone de la plataforma Kaspersky para la protección antivirus de su datacenter, servidores y puestos de trabajo ofimáticos.

Kaspersky, respecto a otros fabricantes:

- es pionero en la protección frente a código malicioso en entornos virtuales, este tipo de entornos representa aproximadamente el 80% de nuestra planta,
- aporta además facilidades para simplificar los procesos de gestión, minimizando el impacto en recursos (menos intrusivo), esto ha permitido una mayor automatización con lo que se agiliza la detección y la respuesta,
- eleva el nivel de protección ya que la infraestructura es core por ser el vector de entrada para cualquier ciberataque,
- dispone de compatibilidad absoluta con la plataforma Hypervisor de RTVM (Vmware Vsphere) e incrementa significativamente la protección a la vez que conserva el rendimiento de cada máquina virtual. RTVM dispone de infraestructura On Premise con tecnología de Hypervisor Vmware Vsphere, donde se aloja el ERP ECO_FIN que soporta procesos económico-financieros, el ERP de RRHH e infraestructura que soporta procesos de negocio como el sistema de producción audiovisual HIVE, AVID Newsroom, los sistemas que dan soporte a los procesos de grafismo y postproducción, AVID Maestro , así como las aplicaciones propias, SIGMA, o de terceros, que se encargan de las integraciones de los procesos de gestión de los materiales audiovisuales (descarga, ingesta, catalogación, distribución, documentación y emisión).

El servicio actual finaliza el próximo 31 de julio de 2026, por tanto, se hace necesario:

- Renovar los derechos de uso de las licencias y el mantenimiento del fabricante.
- Renovar el servicio de soporte.

RTVM pretende, renovar por un periodo de 5 años, el servicio gestionado de antivirus de acuerdo al esquema actual, manteniendo:

- la suite de Kaspersky desplegada en RTVM, homologada, por su compatibilidad con los sistemas de Negocio, que requieren un plataformado específico que condiciona los procedimientos de robustecimiento y militarización y por tanto las herramientas sobre los que se soportan.
- el servicio de remediación de puesto de trabajo y servidores (NeuShield) con el que se ha reforzado la seguridad en el marco del servicio actual ante el crecimiento de las amenazas persistentes en internet con propagación a través de correo electrónico, redes sociales y acceso a internet.

- **Número de Licencias:**
 - Puesto de trabajo: 713.
 - Servidores: 275.
 - Equipos reacondicionados: 300 a partir del 14 de octubre de 2027
 - Servicio de Remediación:
 - Plataforma antiransomware NeuShield: 275 servidores
 - Kaspersky Endpoint Detection and Response Optimum: 713 puestos.
 - Kaspersky Endpoint Detection and Response Optimum adicionales a partir del 14 de octubre de 2027: 300.
- **Nivel de licencia Advance**, con más capacidades de control, hardening, parcheo y cifrado que una licencia estándar.
- **Soporte MSA Plus del fabricante**, es un servicio de soporte técnico Premium ampliado (Maintenance Service Agreement Plus) que ofrece soporte prioritario y especializado, por encima del soporte estándar incluido con las licencias.
- **Servicio de soporte y mantenimiento.**
 - Servicio de soporte técnico, consistente en la realización del primer nivel de servicio para el diagnóstico y resolución de la incidencia, asistencia técnica en caso de incidencia sobre la plataforma central de gestión de Kaspersky así como nuevas instalaciones de producto.
 - Incluye acceso remoto a plataforma de gestión centralizada e intervenciones presenciales en caso de incidencias graves.
 - Horario de resolución de incidencias de forma remota 5x8.
 - Horario de intervenciones presenciales: de 9:00 a 19:00, de lunes a viernes no festivos.
- **Bolsa de 60 horas para soporte a incidencias**, que se consideran de consumo bajo demanda.
- **Bolsa de 60 horas para soporte al proceso de gestión: nuevas políticas, mejoras, cobertura nuevas necesidades**, que se consideran de consumo bajo demanda.

3. SERVICIO DE SOPORTE Y MANTENIMIENTO

El mantenimiento de las licencias incluye el suministro de las nuevas versiones de los productos, así como las actualizaciones de los mismos durante el período contratado. Dichas versiones del producto y actualizaciones estarán accesibles a través de la web del fabricante y se podrán descargar de forma manual o de manera automática mediante las utilidades de actualización que incluya el propio software.

El licitador deberá especificar en su oferta las condiciones del soporte indicando el procedimiento completo de gestión, tiempos de respuesta, franja horaria.

Prestación del servicio

- El licitador proveerá de un número de teléfono en horario 8x5, atención en castellano, para las llamadas que realicen los usuarios de RTVM al centro de soporte (CAU).
- El licitador dimensionará y establecerá una línea de conexión de datos con RTVM a través de una VPN, con redundancia. Toda la infraestructura necesaria, tanto hardware como software o de comunicaciones, correrá a cargo del adjudicatario, que deberá implementar las medidas de seguridad oportunas para garantizar la confidencialidad, integridad y disponibilidad de la información.

- RTVM debe tener posibilidad de reportar un número ilimitado de incidencias y de consultas.
- RTVM debe recibir avisos cuando surjan alertas de seguridad.
- El proveedor debe ofrecer un servicio de verificación, periódico, consistente en la revisión de la configuración y el estado de la plataforma de seguridad implantada, con el fin de comprobar la correcta instalación de todos los productos, así como su correcto funcionamiento y, en su caso, recomendación de posibles mejoras. Se requiere, al menos, la realización de una sesión de verificación anual.
- En caso de detectarse una infección masiva, RTVM solicitará que el adjudicatario desplace un técnico a las instalaciones para ayudar en las tareas de eliminación de la infección.
- Gestión del servicio: RTVM espera mensualmente un informe de seguimiento y control, donde se especifique el grado de cumplimiento de los niveles de servicio, así como los hechos relevantes del periodo.
- Gestión Incidencias: RTVM considera que la gestión de una incidencia debe siempre concluirse con un informe donde se especifique al menos, la causa de la incidencia, el procedimiento operativo que se ha seguido para mitigar el impacto, acciones de mejora etc.

Adicionalmente, durante la duración del contrato, el licitador deberá:

- Dar cobertura a necesidades formativas y/o sesiones orientadas a la transferencia de conocimientos al personal técnico de RTVM.
- Proporcionar toda la documentación técnica del sistema, así como la de las configuraciones instaladas.

El licitador deberá identificar un Gestor del Contrato y un Responsable de Servicio que serán los interlocutores con el Responsable del Servicio de RTVM:

- Gestor del Contrato:
 - Experiencia demostrada de más 8 años.
 - Gestión de al menos tres servicios con el mismo alcance al solicitado.
- Responsable del Servicio:
 - Experiencia demostrada de más 4 años.

Respecto al equipo técnico, será responsabilidad del adjudicatario dimensionar y gestionar al equipo para asegurar los niveles de servicio comprometidos.

4. NIVELES DE SERVICIO Y PENALIZACIONES

Incidencias:

Indicadores relacionados con el parque ofimático

SLA	Criticidad		
	Alta	Media	Baja
Tiempo de respuesta	30 minutos	30 minutos	30 minutos
Tiempo de reacción	30 minutos	2 horas	4 horas
Tiempo de resolución	4 horas	6 horas	Siguiente día laborable

- Alta: 30% del parque ofimático con infecciones, amenazas y/o vulnerabilidades
- Media: 15% del parque ofimático con infecciones, amenazas y/o vulnerabilidades
- Baja: 5% del parque ofimático con infecciones, amenazas y/o vulnerabilidades

Indicadores relacionados con servidores físicos y/o virtuales

SLA	Criticidad		
	Alta	Media	Baja
Tiempo de respuesta	30 minutos	30 minutos	30 minutos
Tiempo de reacción	30 minutos	2 horas	4 horas
Tiempo de resolución	4 horas	6 horas	Siguiente día laborable

- Alta: 30% Servidores físicos y/o virtuales con infecciones, amenazas y/o vulnerabilidades
- Media: 15% Servidores físicos y/o virtuales con infecciones, amenazas y/o vulnerabilidades
- Baja: 5% Servidores físicos y/o virtuales con infecciones, amenazas y/o vulnerabilidades

Peticiones:

Indicadores relacionados con el parque ofimático

SLA	Respuesta
Tiempo de respuesta	8 horas
Tiempo de reacción	8 horas
Tiempo de resolución	2 días laborables

Indicadores relacionados con servidores físico y/o virtuales

SLA	Respuesta
Tiempo de respuesta	2 horas
Tiempo de reacción	4 horas
Tiempo de resolución	Siguiente día laborable

Indicadores relacionados con la plataforma de gestión

SLA	Respuesta
Tiempo de respuesta	2 horas
Tiempo de reacción	4 horas
Tiempo de resolución	Siguiente día laborable

Servicio Gestionado:

Categoría	Tipo de SLA	SLA Objetivo	% Penalización
Accesibilidad al Servicio	Disponibilidad del servicio (vía telefónica, mail, web)	95%	2%
	% de llamadas atendidas	90%	2%
Gestión de Incidencias	Alta	98%	2%
	Media	95%	2%
	Baja	90%	2%

Categoría	Tipo de SLA	SLA Objetivo	% Penalización
	Backlog de incidencias pendientes de resolución (calculado en base al % volumen diario de incidencias y no superado en el 90% de los días)	< 40%	2%
	Tasa de reapertura de incidencias	< 20%	2%
Gestión de Peticiones	Tiempo de resolución de peticiones (90% casos)	80 %	2%
	Backlog de peticiones pendientes de resolución	< 30%	2%
Gestión de la Configuración	Aplicación de políticas (4 revisiones anuales)	90%	2%
	Actualizaciones correctas del motor	95%	2%
	Realización de los escaneos programados	95%	2%
Reporting	Cumplimiento de tiempos comprometidos para la entrega de informes	95%	2%

Los SLA propuestos tendrán una vigencia no superior a 6 meses. Con dicha periodicidad, dentro de los **planes de mejora continua** que debe regir el servicio, se valorarán, conjuntamente, los indicadores y los umbrales de servicio comprometidos, estableciéndose nuevos objetivos de mejora y, en consecuencia, se podrían incluir o retirar SLAs.

El cálculo de los indicadores y de las correspondientes penalizaciones se realizará mensualmente y, esa información debe siempre incluirse en el informe mensual de seguimiento y control del servicio.

Para cada uno de los indicadores (de los propuestos en el pliego por RTVM y de los que puedan surgir a lo largo del contrato), se establece una penalización, con un tope del 20% de la facturación mensual total. El incumplimiento prolongado durante más de 2 meses de dos o más niveles de servicio (SLAs) será causa de rescisión del contrato. Esta penalización no se aplica de forma escalonada, sino para todos los SLA:

Nº SLA incumplidos	Penalización - % importe facturación mensual
Menos de 3 SLA	2% por SLAs/mes
Entre 3 y 5 SLA	5% por SLA/mes
Más de 5 SLA	8% SLA /mes

5. CONTENIDO DE LAS OFERTAS TÉCNICAS

Con independencia de que el licitador pueda adjuntar a su oferta cuanta información complementaria considere de interés:

- La memoria técnica no deberá extenderse a más de **30 páginas**. El no cumplimiento de este **requerimiento es motivo de exclusión**. La información adicional que se considere incluir, se presentará en documentos separados.

Adicionalmente:

1. De conformidad con lo establecido en el artículo 133 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, los licitadores podrán designar como confidencial aquella información de su oferta cuya divulgación pueda perjudicar sus intereses comerciales legítimos, como secretos técnicos o comerciales.
2. **Bajo ningún concepto se admitirá la declaración de confidencialidad sobre la totalidad de la memoria técnica o de cualquier otro documento que forme parte de la oferta.** La información que sea objeto de valoración según los criterios de adjudicación debe ser, en principio, accesible al resto de licitadores en aras de la transparencia del procedimiento.
3. En caso de que el licitador considere que alguna parte de su oferta posee carácter confidencial, deberá:
 - **Identificar y señalar con precisión** qué documentos, apartados, datos o información específicos considera confidenciales.
 - **Presentar dicha información debidamente separada** o claramente delimitada dentro de la memoria técnica (o en un documento aparte referenciado, si la plataforma de contratación lo permite).
 - **Justificar de forma suficiente y detallada** los motivos por los que dicha información tiene valor estratégico, no es pública y su divulgación le causaría un perjuicio económico o comercial grave. Una simple declaración genérica no será suficiente.

La Memoria Técnica donde se describa las condiciones del soporte y mantenimiento debe responder a la siguiente estructura:

- Descripción del servicio;
- Plan de Trabajo;
- Procedimientos Operativos;
- Gestión de Incidencias;
- Seguimiento y control;
- Aseguramiento de la calidad: mejora continua.

Firmado digitalmente por
SUBDIRECTORA SISTEMAS -
RTVM22597 - RADIO TELEVISION
MADRID. Fecha: 14/01/2026.