Pliego de condiciones técnicas para la renovación del paquete de licencias del software antivirus Kaspersky, así como su mantenimiento, para la Agencia Pública Empresarial de la Radio Televisión de Andalucía y Canal Sur Radio y Televisión, S.A. (RTVA y CSRTV)

1 Objeto

El objeto de este pliego es establecer las condiciones técnicas que regirán la contratación de la renovación del paquete de licencias del software antivirus Kaspersky Security for Business Advanced, así como su mantenimiento, en uso en RTVA. Actualmente este software se encuentra descatalogado, habiendo evolucionado a la solución Kaspersky Next Optimum, por lo que serán de este producto las licencias a facilitar su uso.

Desde el punto de vista de la contratación, el objeto incluye el suministro de 1600 licencias de Kaspersky Next Optimum, así como un servicio de mantenimiento posterior que incluye un soporte remoto. Se trata, por tanto, de un contrato mixto, aunque el mayor peso económico lo tiene el suministro.

2 Licencias actuales

Actualmente RTVA dispone de un total de **1.600** licencias en uso de la versión Kasperky Security for Business en su modalidad ADVANCED cuyo vencimiento se ha producido el pasado 9 de febrero de 2026, habiéndose tramitado un expediente de contratación menor para mantener la vigencia de dichas licencias hasta que entre en vigor el presente expediente de contratación. Resulta necesario contratar su continuidad.

3 Renovación de la suscripción y servicios de mantenimiento

El presente pliego se refiere a la renovación y mantenimiento por un periodo de tres (3) años de la suscripción de **1.600** licencias del software antivirus Kaspersky Next Optimun.

La plataforma de protección debe tener un servicio de soporte personalizado para RTVA, certificado por el fabricante, siendo imprescindible tener un conocimiento detallado del sistema implantado en RTVA.

El presente pliego contemplará los siguientes servicios:

Un mínimo de dos (2) consolas para administración y control, que permitan la administración separada desde diversas áreas técnicas, sin que se produzca conflicto, y se mantenga la independencia de cada administración.

- Suscripción por tres (3) años de 1.600 licencias para protección antivirus de clientes y servidores.
- Acceso a las actualizaciones de versión y mejoras del producto, así como a la actualización de la base de datos de virus.
- Prestación de un servicio de soporte personalizado y específico para RTVA, que permita a los técnicos de RTVA disponer de un programa de asistencia, tratando problemas de seguridad con una alta prioridad y manteniendo el negocio en marcha.
- Servicios profesionales en remoto para asistencia en la instalación o actualización de versiones, realizado por especialistas certificados de las soluciones de Kaspersky. Seguirán las mejores prácticas y metodologías recomendadas en la implementación y optimización de la solución. Este servicio ofrecerá asistencia en:
    - Evaluaciones, auditorías y análisis del estado de la seguridad
    - Implementaciones y configuración de la seguridad de la plataforma

- Mantenimiento y soporte integral con posibilidad de acceso
- Kasperky Maintenance Agreement Plus (3 años)
- Kaspersky Professional Services (8 horas anuales en remoto)

4 Duración del contrato

El plazo de ejecución de la presente contratación será, a partir de la aceptación de la adjudicación, de tres (3) años a contar desde la puesta en servicio efectivo de las nuevas licencias, en un plazo máximo de un mes y previa acta de conformidad de RTVA, sin posibilidad de prórroga.

5 Documentación a entregar una vez finalizado el suministro

Certificado de las licencias incluidas en la oferta.

6 Precio máximo y Forma de pago

Se establece un precio máximo de 53.955 € (Cincuenta y tres mil novecientos cincuenta y cinco euros), IVA no incluido.

IVA 21%: 11.330,55 € (once mil trescientos treinta euros con cincuenta y cinco céntimos)

Total presupuesto base de licitación, IVA incluido: 62.285,55 € (Sesenta y dos mil doscientos ochenta y cinco euros con cincuenta y cinco céntimos)

Desglose de precios (IVA no incluido):

- Kaspersky Next Optimum (1.600 licencias para 3 años) 7,5€ * 1600 * 3 años = 36.000 €
- Kaspersky Maintenance Service Agreement, Plus 5.250 € x 3 años = 15.750 €
- Kaspersky Professional Service -8 Hours, asistencia remota 735 € x 3 años = 2.205 €

El pago se hará anualmente, a razón de una tercera parte del precio de adjudicación, previa la presentación de las correspondientes facturas en el Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado (FACE) y con la conformidad de RTVA al suministro, una vez completadas todas las obligaciones incluidas en el alcance de la contratación.

7 Criterios de adjudicación.

El único criterio de valoración será el precio ofertado. La adjudicación recaerá sobre la oferta válida con el precio ofertado más bajo.

8 Condiciones generales

8.1 Confidencialidad de la información

La información a la que tenga acceso la empresa como consecuencia del contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de RTVA.

8.2 Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información dictados por el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación. Para lograr esto, se adoptarán las medidas de seguridad indicadas en el anexo II del ENS aplicables a la **categoría media** del sistema y al **nivel medio** de seguridad de las **dimensiones de confidencialidad**, integridad, trazabilidad, autenticidad y disponibilidad.

A estas medidas se sumarán aquellas medidas adicionales que se definan por el Responsable de Seguridad (artículo 28 del ENS) y aquellas que se añadan en base a análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, a la evaluación de impacto en la protección de datos (artículo 3.3 del ENS).

El Responsable de Seguridad trasladará las medidas aplicables a través del Responsable del Contrato durante la ejecución de este.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la Política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

Se atenderá también a la normativa interna del organismo contratante en materia de ciberseguridad. Deberá respetarse la Política de Seguridad de la Información y Protección de Datos Personales de la RTVA y CSRTV, accesible en el siguiente enlace: https://www.canalsur.es/resources/static/Politica_Seg_Info-PD-RTVA-CSRTV_2023.pdf.

El organismo contratante desplegará los medios necesarios para auditar el cumplimiento de la política de seguridad y de los niveles de servicio acordados por parte del contratista, según lo expresado en los documentos de contratación.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (https://www.ccn-cert.cni.es/es/), así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y a las indicaciones del Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía.

Colaboración en la gestión de la seguridad del sistema

El adjudicatario colaborará con la realización de los análisis de riesgos que se realicen, que tendrán en cuenta los siguientes aspectos:

- Identificación de los activos relevantes dentro del alcance considerado del Sistema de Información.
- Valoración cualitativa de los activos más valiosos del sistema. La valoración de los activos corresponde a los responsables designados en la política de seguridad del organismo. Para ello se tendrá en cuenta el perjuicio que supondría su degradación.
- Identificación y cuantificación de las amenazas más probables.
- Identificación y valoración de las salvaguardas que protegen de dichas amenazas.
- Identificación y valoración del riesgo residual.

El adjudicatario deberá prestar al organismo la colaboración necesaria durante la realización de auditorías técnicas y de cumplimiento normativo.

Certificación ENS de la empresa

En cumplimiento de la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad aprobada por Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, el adjudicatario deberá disponer de Declaración o **Certificación de Conformidad con el ENS categoría media o alta**; para la prestación de los servicios o provisión de las soluciones contempladas en este expediente, en caso de existir en el alcance de esta contratación servicios no prestados desde las instalaciones de la Junta de Andalucía (por ejemplo, servicios prestados desde una nube). Esta Certificación de Conformidad con el ENS debe versar sobre soluciones proporcionadas o servicios prestados por el operador del sector privado que estén relacionadas con las soluciones y servicios que son objeto de contratación del presente expediente, según apartado VII.1 de la Instrucción Técnica de Seguridad citada.

Interlocución y roles en materia de ciberseguridad

Se asignarán los roles relacionados con la seguridad de los sistemas de información, reflejados en el Esquema Nacional de Seguridad y detallados en la guía CCN-STIC 801 (Responsabilidades y Funciones en el ENS).

La interlocución con el adjudicatario en aspectos de seguridad corresponderá al Responsable del Contrato, con la colaboración y con la orientación del Responsable de Seguridad.

Todos estos roles serán identificados e informados, dentro del marco normativo de seguridad establecido en la Junta de Andalucía, desde el inicio del desarrollo del sistema.

Punto de contacto (PoC) de seguridad

En cumplimiento del artículo 13 del Real Decreto 311/2022 (Esquema Nacional de Seguridad), el adjudicatario deberá designar un PoC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de ciberseguridad y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El adjudicatario deberá comunicar cualquier cambio o sustitución de dicho POC a lo largo de la vida del contrato.

Dicho PoC de seguridad será el propio responsable de Ciberseguridad del contratista, formará parte de su área o tendrá comunicación directa con la misma, y su identificación se comunicará al SOC de la Junta de Andalucía a través del Responsable de Seguridad asignado al sistema.

La comunicación de este PoC incluirá la referencia al contrato en el cual se realiza, su duración estimada, las actividades principales a realizar y los accesos remotos que se prevén.

Gestión de incidentes

El adjudicatario comunicará al personal de ciberseguridad del organismo, en primera instancia, o al Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía cualquier ciberincidente que detecte o del que tenga conocimiento.

Para la gestión de los incidentes de seguridad se seguirá lo dictado en la vigente Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC (https://juntadeandalucia.es/boja/2018/141/29). En especial, en el punto 6 (comunicación de

incidentes), 8 (comunicación entre organismos y entidades de incidentes y medidas adoptadas), 9 (colaboración con AndalucíaCERT) y 11 (denuncias).

Accesos remotos

El acceso remoto de los técnicos del equipo del proyecto, en el marco del contrato, a los servicios o sistemas de información de la entidad contratante Agencia Digital de Andalucía, se realizará nominalmente mediante el procedimiento aprobado por la Red Corporativa de la Junta de Andalucía (que podrá incluir, a modo de ejemplo, la opción de cliente VPN y/o soluciones de tipo SASE) sin necesidad de disponer de una conexión permanente al Nodo de Interconexión de la Red Corporativa de la Junta de Andalucía (funcionamiento en modo cliente de servicios internos, esto es, conectividad no simétrica), previa autorización por parte del Responsable del Contrato. Caso de que algún software necesario por el adjudicatario para el acceso remoto requiera de suscripción, el adjudicatario se deberá hacer cargo de estos posibles gastos ocasionados.

El modo de acceso será tal que garantice la seguridad de operación y explotación del sistema, así como el objetivo de almacenar y gestionar las solicitudes de servicio e incidencias que se produzcan durante la ejecución del contrato.

El adjudicatario debe realizar las solicitudes de forma individual para cada uno de los técnicos que requieran el acceso remoto, debiendo ser validada cada solicitud por el Responsable del Contrato. Asimismo, deberá comunicar en su caso las bajas eventuales que pudiera producirse durante la vida del contrato.

El adjudicatario debe cumplir con la política de acceso remoto que aplique en el organismo durante todo el periodo de vigencia del contrato, que puede incluir, entre otros aspectos: alta del usuario en el Directorio Corporativo de la Junta de Andalucía, mecanismo de identificación y autenticación robusto empleando el certificado digital de la FNMT, software de la red privada virtual a utilizar, funciones permitidas y datos accesibles desde acceso remoto, tiempo máximo para cerrar sesiones inactivas, activación de los registros de actividad, etc.

Igualmente, el adjudicatario asegurará que la comunicación esté limpia de malware, virus y/o cualquier otro tipo de tráfico malicioso o no deseado.

Requisitos de seguridad en el desarrollo de aplicaciones

Se deberán considerar al menos los siguientes requisitos de seguridad, en el caso de que el objeto del contrato implique trabajos de desarrollo:

- Defensa en profundidad, estableciéndose distintos puntos de control de seguridad en las distintas capas de una aplicación.
- Confidencialidad en las comunicaciones.
- Avisos legales sobre deberes y obligaciones.
- Prevención ante la obtención de credenciales de usuarios.
- Posibilidad de inhabilitación de cuentas de usuario.
- Se garantizará el principio de mínimo privilegio, tanto en el acceso a los datos como a las funciones. La gestión de estos permisos se realizará a través de roles, evitando la posibilidad de asignar permisos o privilegios directos.
- Identificación unívoca de usuario registrado.
- Autenticación y gestión de sesiones de forma segura con objeto de evitar el robo o la manipulación de sesión.
- Trazabilidad.
- Validación de datos de entrada y salida.
- Gestión correcta de mensajes de error.
- Gestión segura de archivos.

- Limpieza de documentos creados o publicados por el aplicativo.

8.3 Sobre la gestión de usuarios y el control de accesos

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) así como de la legislación nacional vigente en materia de protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), y el Real Decreto 311/202, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En particular, se perseguirá:

- la correcta identificación de los usuarios (medida op.acc.1 del anexo II del ENS).
- la correcta gestión de los requisitos de acceso (medida op.acc.2).
- segregación de funciones y tareas (medida op.acc.3).
- la adecuada gestión de derechos de acceso (medida op.acc.4).
  la correcta selección e implantación de los mecanismos de autenticación, tanto para usuarios de la organización como usuarios externos a la organización (medidas op.acc.5 y op.acc.6).

a) En relación con las directrices corporativas que se creen en materia de gestión de identidades.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar (roles, gestión de credenciales...) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta haya provisto. Dichas directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

b) En el caso de que, en alguno de los sistemas, aplicaciones, herramientas, etc. objeto de contratación se gestionen trámites y actuaciones que se realizan con la Administración de la Junta de Andalucía por razón de la condición de empleado público.

El sistema deberá admitir, para los trámites y actuaciones que su personal realice con ella por razón de su condición de empleado público, el sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA) de acuerdo con el artículo 25.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.