PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO SIMPLIFICADO DE TRAMITACIÓN ABREVIADA, DE LA RENOVACIÓN DE LICENCIAS DE DOS EQUIPOS CORTAFUEGOS (FIREWALLS), EN ALTA DISPONIBILIDAD, DE LA AGENCIA ANDALUZA DE COOPERACIÓN INTERNACIONAL PARA EL DESARROLLO.

EXPDTE. CONTR 2026 302705

1. INTRODUCCIÓN

La Agencia Andaluza de Cooperación Internacional para el Desarrollo, en adelante AACID, tiene como objetivo para los próximos años continuar avanzando en el proceso de Transformación Digital, teniendo como uno de los principales ejes de actividad la modernización del puesto de trabajo de las personas usuarias, impulsando la movilidad y la capacitación en competencias digitales.

Con objeto de renovar tecnológicamente la capa de seguridad perimetral de la sede de la AACID, a finales del año 2023 la Agencia adquirió dos equipos cortafuegos (firewalls) Check Point Quantum Spark 1600 Appliance, configurados en alta disponibilidad.

Estos equipos proporcionan protección a las infraestructuras TIC ubicadas en la sede de la Agencia frente al resto de la Red Corporativa de la Junta de Andalucía. Esta protección comprende tanto la red interna a la que se conectan las personas usuarias y los distintos dispositivos corporativos —ordenadores portátiles, teléfonos IP, impresoras, etc.— como la infraestructura propia alojada en la sala técnica de la sede, desde la que se prestan diversos servicios auxiliares al puesto de trabajo, entre ellos el servidor secundario de ficheros y los servicios de acceso remoto mediante RDS.

Las licencias asociadas a ambos equipos cortafuegos expiran el próximo 9 de enero de 2027. La vigencia de estas licencias resulta necesaria para mantener actualizados los mecanismos de protección de los equipos, disponer de las correspondientes actualizaciones de seguridad y nuevas versiones de firmware, así como contar con el soporte especializado del fabricante ante posibles incidencias o averías.

Por tanto, con el fin de garantizar la continuidad y eficacia de las medidas de seguridad perimetral y mantener adecuadamente protegidas las infraestructuras y los servicios TIC prestados desde la sede de la Agencia, resulta necesaria la renovación de las licencias asociadas a ambos equipos cortafuegos.

2. OBJETO Y ALCANCE

El alcance de lo especificado en esta contratación comprende la renovación de las licencias de dos equipos cortafuegos (firewalls) Check Point Quantum Spark 1600 Appliance, configurados en alta disponibilidad, en una modalidad de soporte Premium Enterprise para 36 meses.

La empresa adjudicataria deberá proveer a la AACID la renovación de las licencias objeto de este contrato, así como garantizar los derechos de licencia y utilización de las nuevas versiones de dicho software en cuanto sean liberadas por el fabricante.

Junta de Andalucía

3. DESCRIPCIÓN Y CARACTERÍSTICAS DE LAS LICENCIAS

En la actualidad, la AACID cuenta con dos equipos cortafuegos (firewalls) Check Point Quantum Spark 1600 Appliance, configurados en alta disponibilidad:

Equipo	Número de serie
FW01	BA23803074
FW02	BA23803076

Y con el siguiente licenciamiento:

Software	Expiración	Servicio
Firewall	Nunca	CPSB-FW
Application Control	09/01/2027	CPSB-APCL-S-2Y
URL Filtering	09/01/2027	CPSB-URLF-S-2Y
User Awareness	Nunca	CPSB-IA
QoS	Nunca	CPSB-ADNC-SMB
Intrusion Prevention (IPS)	09/01/2027	CPSB-IPS-S-2Y
Anti-Virus	09/01/2027	CPSB-AV-S-2Y
Anti-Bot	09/01/2027	CPSB-ABOT-S-2Y
Threat Emulation	09/01/2027	CPSB-TE-S-2Y
Anti-Spam	09/01/2027	CPSB-ASPM-S-2Y
Site to Site VPN	Nunca	CPSB-VPN

La fecha de entrada en vigor del uso de las licencias sujetas a renovación fue el 10/01/2024 y se extenderá hasta el 09/01/2027, por lo que resulta necesaria su renovación con efectos desde el 10/01/2027, y por un periodo de 36 meses y con un nivel de soporte Premium Enterprise.

Del mismo modo, los dos equipos cortafuegos (firewalls) Check Point Quantum Spark 1600 Appliance disponen de dos transceivers Check Point CPAC-TR-1SX-C cuyo periodo de mantenimiento y soporte comenzó con anterioridad al uso de las licencias:

Componente	Número de serie
Transceiver 1	CPT165718539
Transceiver 2	CPT165718544

La fecha de entrada en vigor del mantenimiento y soporte de los transceivers fue el 18/11/2023 y se extenderá hasta el 17/11/2026, por lo que resulta necesaria su renovación con efectos desde el 18/11/2026 hasta el 09/01/2030, de forma que su fecha de finalización quede alineada con la correspondiente a las licencias de los equipos cortafuegos.

Junta de Andalucía

Por último, la empresa adjudicataria se encargará de todas las tareas necesarias para la activación en los equipos cortafuegos (firewalls) de las nuevas licencias objeto del presente contrato.

4. CONDICIONES GENERALES DEL SUMINISTRO

4.1. LUGAR DE REALIZACIÓN

Por petición del responsable del contrato y para la óptima realización del proyecto, existe la posibilidad de que algunos trabajos se deban desarrollar en instalaciones o edificios de la AACID.

4.2. PROPIEDAD INTELECTUAL DE LOS TRABAJOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de la AACID, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este documento de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la AACID. Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de este contrato corresponden únicamente a la Agencia.

La presente cláusula no se aplicará a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

4.3. CUMPLIMIENTO DEL ESQUEMA NACIONAL DE 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 del sistema y a los niveles de seguridad requeridos para el mismo, en las dimensiones de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad, que se detallan a continuación: categoría de seguridad BÁSICA.

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.

Junta de Andalucía

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.

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 (http://www.ccn-cert.cni.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.

4.4. 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.

4.5. 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 Certificación de Conformidad con el ENS categoría 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.

Caso de que el adjudicatario no disponga de la Certificación de Conformidad indicada, se le otorgaría un plazo máximo de 6 meses para la obtención de ésta, contados a partir de la fecha de adjudicación/formalización del contrato.

4.6. 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.

4.7. 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.

4.8. 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.

Junta de Andalucía

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).

4.9. 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 AACID, 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.

4.10. TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL

La empresa suministradora, en cumplimiento de lo previsto en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, únicamente tratará los datos conforme a las instrucciones de la AACID, y no los aplicará o utilizará con fin distinto al del contrato; ni los comunicará, ni siquiera para su conservación, a otras personas.

Junta de Andalucía

4.11. CONFIDENCIALIDAD

La empresa adjudicataria se obliga a guardar el debido sigilo profesional de cuanta información tenga conocimiento para cumplimiento del presente servicio, tratará los datos conforme a las instrucciones de la AACID y no los aplicará o utilizará con fin distinto, ni los comunicará o cederá, ni siquiera para su conservación, a otras personas. Además, deberá cumplir las medidas estipuladas en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. De igual modo, el adjudicatario se compromete a no conservar copia alguna de información personal, y destruir o devolver por tanto los datos facilitados por esta Agencia, una vez finalizada la vigencia del presente contrato. Cuando, por el contrario, el cumplimiento del objeto del servicio no requiera el acceso por parte del adjudicatario a datos de carácter personal, se prohíbe expresamente dicho acceso y, si por cualquier causa tuviere lugar, se establece la obligación de secreto respecto a los datos que se hubieran podido conocer con ocasión de su ejecución.

4.12. COSTES DEL SUMINISTRO

El presupuesto total con impuestos incluidos para la renovación de licencias descrita en el presente documento es de SIETE MIL CIENTO OCHO EUROS (7.108 €).

La Jefatura de Tecnología y Estrategia Digital de la Agencia Andaluza de Cooperación Internacional para el Desarrollo
Fdo.: Miguel Ballesteros Cáliz