ATM Àrea de Barcelona
Autoritat del Transport Metropolità

Pliego de prescripciones técnicas para a la contratación por procedimiento abierto sujeto a regulación armonizada del suministro:

«Herramientas Ciberseguridad»

(Exp. C-4/2026)

Junio 2026

ÍNDICE

1. PRESCRIPCIONES GENERALES

Este Pliego de prescripciones técnicas tiene por objeto determinar el contenido y el alcance de los suministros que deberá proporcionar la empresa contratista y los requisitos que debe cumplir para ser adjudicataria de la misma.

Con este objetivo se describen los suministros a proporcionar y se relacionan las materias que deben servir de base para licitar y garantizar la calidad de las propuestas.

Asimismo, se describen las características y contenido de las ofertas a presentar y los criterios que servirán de base, tanto para la adjudicación de los trabajos como para que los mismos sean aceptados por la dirección de la asistencia técnica.

La dirección de los servicios y su aprobación dependerán del Área de Sistemas e Innovación de la Autoridad del Transporte Metropolitano, Consorcio para la coordinación del sistema metropolitano de transporte público del Área de Barcelona (en adelante, ATM).

Con la mera presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

2. DESCRIPCIÓN DE LOS TRABAJOS

2.1 Antecedentes

La Autoridad del Transporte Metropolitano del área de Barcelona (en adelante ATM) es un consorcio interadministrativo de carácter voluntario creado en 1997. Actualmente, las administraciones consorciadas son la Generalitat de Cataluña (51 %) y administraciones locales (49 %), compuestas por el Ayuntamiento de Barcelona, el Área Metropolitana de Barcelona (anteriormente denominada Entidad Metropolitana del Transporte) y la Asociación de Municipios para la Movilidad y el Transporte Urbano (AMTU), a la cual se pueden adherir todas las administraciones titulares de servicios públicos de transporte colectivo que pertenezcan al ámbito formado por las comarcas del Alt Penedès, la Anoia, el Bages, el Baix Llobregat, el Barcelonès, el Berguedà, el Garraf, el Maresme, Osona, el Vallès Occidental y el Vallès Oriental. Además, la Administración General del Estado está presente en los órganos de gobierno de la ATM en calidad de observador.

El Área de Sistemas e innovación tiene encomendadas, entre otros aspectos, la gestión de las políticas de seguridad informática y de protección de datos, la de los sistemas de seguridad en red y la de los sistemas corporativos de autenticación de usuarios. Esta Dirección administra una infraestructura de comunicaciones y servidores que proporciona el soporte sobre el que se implementan las aplicaciones corporativas, se distribuye la información de sus servicios y se prestan los servicios telemáticos a los ciudadanos. En consonancia con el principio básico de «Líneas de defensa» establecido en el Real Decreto 311/2022 del 3 de mayo, por el cual se regula el Esquema Nacional

de Seguridad (ENS), para asegurar estas comunicaciones hay que orientar la estrategia de seguridad hacia una solución de arquitectura multicapa, consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de que los sistemas de información se vean comprometidos y minimizar el impacto si la situación de riesgo llega a materializarse.

Para mejorar la seguridad y la calidad del servicio prestado al ciudadano se requiere mantener esta capa de protección en la infraestructura de la web corporativa, renovando la solución WAF existente. Este sistema de seguridad se aplica a los accesos que pretendan hacer uso de aplicaciones o servicios web, analizando el tráfico correspondiente, detectando y bloqueando el tráfico malicioso antes de que llegue a su destino. Asimismo, la ATM quiere dotar a esta solución ya existente de un sistema de protección contra bots que puedan atacar a sus aplicaciones expuestas en Internet.

A raíz de la implementación de la T-mobilitat, la ATM ha puesto a disposición de la ciudadanía unos canales telemáticos de comunicación con el objetivo de que los ciudadanos puedan darse de alta en el sistema y también gestionar sus cuentas de usuario y adquirir nuevos títulos de transporte.

Estas nuevas funcionalidades implican la exposición de portales y aplicaciones que permiten cursar estas solicitudes, para lo cual es necesario disponer de las licencias WAF vigentes que permitan proteger las aplicaciones web al filtrar y monitorizar el tráfico HTTP entre una aplicación web e internet. Asimismo, estas aplicaciones y portales pueden ser vulnerables a la programación de bots. Estas redes de bots generan peticiones ilícitas de forma automatizada y recurrente, con el objetivo de acceder de forma no autorizada a información no pública o bien causar una disrupción del servicio.

Asimismo, teniendo en cuenta que los ataques por correo electrónico son cada vez más complejos y peligrosos, se pretende renovar el servicio de protección antivirus para Microsoft 365, con el fin de seguir manteniendo la protección ante amenazas de correo electrónico, desde *spam* y el *ransomware*, hasta las amenazas de ingeniería social como *spear phishing*, entre otros.

Por otro lado, también se considera necesario mantener la seguridad de los servicios expuestos en Internet, así como disponer de información sobre el uso de las marcas ATM, en prevención del *phishing* y otras actividades que puedan deteriorar la reputación de la ATM, finalidades que se lograrán con la adquisición de una solución EASM (External Attack Surface Management).

Finalmente, con el objetivo de optimizar la seguridad y la productividad de la ATM, se requiere renovar el soporte técnico del fabricante Fortinet de la plataforma de seguridad con los elementos que actualmente tiene la ATM.

La ATM ha sido víctima de todas estas prácticas ilícitas que han tenido su correspondiente impacto en la calidad del servicio prestado. En consecuencia, han puesto de manifiesto que la carencia de estas herramientas de protección en este sentido está exponiendo a los sistemas y los servicios de la ATM a sufrir impactos y que incluso estos ataques puedan pasar inadvertidos o interpretarse como una simple

disminución del rendimiento, de modo que el riesgo para la seguridad de los servicios no está actualmente a un nivel aceptable.

En el presente Pliego de Prescripciones Técnicas se describen las necesidades al respecto.

2.2 Objeto del contrato

El objeto del contrato es el suministro de licencias de soluciones en materia de ciberseguridad.

La finalidad de la contratación es disponer de unas capas de protección de ciberseguridad ante posibles ataques e intrusiones. Concretamente en este contrato se contempla la protección de portales con WAF, Antibot, DDos y Web DDos; protección del correo electrónico; análisis de superficies de ataque externas (EASM), y licencias firewalls.

Estos elementos de seguridad están actualmente implantados en la ATM. El objetivo de la presente licitación es garantizar la continuidad de los servicios y soluciones de seguridad contratadas mediante los expedientes de licitación C-37/2022 «Herramientas de ciberseguridad» y C-31/2023 «Herramientas de ciberseguridad (Fase II)» actualmente en vigor.

El objeto del contrato se divide en los siguientes lotes:

- Lote 1: Renovación Licencias Servicio Cloud Radware
- Lote 2: Renovación Licencias Barracuda
- Lote 3: Renovación Licencias Fortirecon
- Lote 4: Renovación Licencias Firewalls Fortinet

2.3 Actividades y funciones de la empresa adjudicataria

El suministro regulado en este pliego debe ajustarse, al menos, a los requisitos técnicos especificados en este Pliego, sin perjuicio de los parámetros que deben valorarse mediante los criterios de adjudicación establecidos.

La empresa contratista debe disponer de los suficientes medios técnicos y materiales cualitativos para desarrollar las tareas objeto del correspondiente contrato. Se valorará el nivel de partenariado de la empresa adjudicataria con el fabricante.

El suministro deberá cumplir con los parámetros de calidad y seguridad establecidos por la ATM, la legislación vigente y las principales normas y buenas prácticas aplicables en las tecnologías de la información y la comunicación, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información a la que pueda tener acceso el adjudicatario en virtud del contrato.

La oferta que presente la empresa licitadora deberá abarcar los suministros especificados en cada uno de los lotes del presente pliego y en el Pliego de Cláusulas

Administrativas Particulares, siendo todas ellas obligatorias para la admisión de las propuestas.

Los suministros que deberá realizar la empresa adjudicataria son los siguientes:

a) <u>Lote 1: Renovación Licencias Servicio Cloud Radware</u>

Para poder mantener la protección de los portales actuales serán necesarias las licencias descritas a continuación:

- Radware Cloud Application Protection Service Complete
- 5 apps de la herramienta Radware Cloud WAF Enterprise
- 5 licencias de la herramienta Radware Bot Manager's Anti-Bot Solution
- Paquete Bot Manager Analytics Add-donde for Cloud Application
- Paquete de 50Mb con 5 Apps de la herramienta Radware Cloud Web DDoS
- Paquete Access Logs – Visibility and Export

El suministro del software indicado debe ir acompañado de:

- Gestión de las licencias, instalación, configuración, mantenimiento en su operación y la gestión de incidencias relacionadas con las herramientas contratadas, no en su gestión del día a día.
- Período de habilitación de las licencias mínimo de 3 años.
- Soporte 24x7 del producto.
- Capacitación y soporte: se requiere que la herramienta proporcione capacitación y soporte tipo Completo del fabricante, para ayudar a la ATM a mantener el sistema.

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si esta se convierte en la adjudicataria.

b) <u>Lote 2: Renovación Licencias Barracuda</u>

Para poder mantener la protección de los entornos Microsoft 365 actuales serán necesarias las licencias descritas a continuación:

- Barracuda Email Protection Premium Plus para un total de 180 usuarios.

Otras características a cumplir:

- Gestión de las licencias, instalación, configuración, mantenimiento en su operación y la gestión de incidencias relacionadas con las herramientas contratadas, no en su gestión del día a día.
- Período de habilitación de las licencias mínimo de 3 años.
- Soporte 24x7 del producto.

- Capacitación y apoyo: se requiere que la herramienta proporcione capacitación y soporte tipo Premium del fabricante, para ayudar a la ATM a mantener el sistema.

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si esta se convierte en la adjudicataria.

c) <u>Lote 3: Renovación Licencias Fortirecon</u>

Para poder mantener la revisión de la superficie de ataque externa (EASM) es necesario renovar las licencias actuales:

- Fortirecon External Attack Surface Monitoring & Brand Protect up to 500 monitored assets.

Otras características a cumplir:

- Gestión de las licencias, instalación, configuración, mantenimiento en su operación y la gestión de incidencias relacionadas con las herramientas contratadas, no en su gestión del día a día.
- Período de habilitación de las licencias mínimo de 3 años.
- Soporte 24x7 del producto.
- Capacitación y soporte: se requiere que la herramienta proporcione capacitación y soporte del fabricante, para ayudar a la ATM a mantener el sistema.

d) <u>Lote 4: Renovación Licencias Firewalls Fortinet</u>

Para poder mantener la protección de los equipamientos Fortinet es necesario renovar las licencias actuales de mantenimiento. Equipos a mantener:

- 2 Firewall modelo FortiGate 200F
- 9 dispositivos FortiAP
- Licencias ZTNA

Otras características a cumplir:

- Gestión de las licencias, instalación, configuración, mantenimiento en su operación y la gestión de incidencias relacionadas con las herramientas contratadas, no en su gestión del día a día.
- Periodo de habilitación de las licencias mínimo de 3 años.
- Soporte 24x7 del producto.
- Capacitación y soporte: se requiere que la herramienta proporcione capacitación y soporte tipo del fabricante, para ayudar a la ATM a mantener el sistema.

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si esta se convierte en la adjudicataria.

3. CALENDARIO DE TRABAJO Y DURACIÓN DEL CONTRATO

Se establece una duración del presente contrato de 3 años, con posibilidad de prórroga por el plazo de un año cada uno de los lotes.

Por cada uno de los lotes las licencias se activarán a partir del momento de la formalización del contrato.

4. CONDICIONES GENERALES DE EJECUCIÓN Y CIBERSEGURIDAD

Todo producto o software de seguridad será evaluado por la organización conforme al ENS. Se priorizarán productos certificados (CPSTIC, CCN-STIC 105 o equivalentes). En ausencia de certificación, se realizará análisis de riesgos, definición de medidas compensatorias y aceptación formal. El adjudicatario deberá aportar la información técnica necesaria y garantizar la seguridad del componente durante su ciclo de vida.

4.1 Principios básicos

- **Deber de confidencialidad.** El personal de la empresa adjudicataria debe mantener absoluta confidencialidad y estricto secreto sobre la información conocida a raíz de la ejecución de los servicios contratados. Esta obligación de confidencialidad tiene carácter indefinido y subsistirá incluso después de haber cesado su relación laboral con la ATM. La empresa adjudicataria debe comunicar esta obligación de confidencialidad a su personal y debe controlar su cumplimiento. La empresa adjudicataria debe poner en conocimiento de la ATM, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar a la integridad o la confidencialidad de la información. Este deber se extiende a los empleados de otras empresas que, a petición del adjudicatario, participen en la prestación de los servicios recogidos en este pliego.

- **Propiedad intelectual:** toda la documentación que se genere durante la prestación de los servicios de soporte es propiedad exclusiva de la ATM.

  Toda la documentación generada en la presente contratación será propiedad de la ATM, no pudiendo hacerse ningún uso de la misma por parte del Adjudicatario, así como de todos los desarrollos realizados dentro de la presente licitación**.**

- **Criterios de accesibilidad universal:** la empresa adjudicataria se responsabilizará de cumplir con los criterios de accesibilidad universal, tal cómo se definen estos términos en el texto refundido de la Ley General de derechos de las personas con discapacidad y de inclusión social, aprobado mediante Real Decreto Legislativo 1/2013, de 29 de noviembre.

Los medios de comunicación, el diseño de los elementos instrumentales y la implantación de los trámites procedimentales empleados por la empresa contratista en la ejecución del contrato deberán realizarse teniendo en cuenta los criterios de accesibilidad universal y de diseño para todo el mundo.

- **Criterios de sostenibilidad y protección al medio ambiente:** la empresa adjudicataria se responsabilizará de cumplir con los criterios de sostenibilidad y protección del medio ambiente, de acuerdo con las definiciones y principios regulados en los artículos 3 y 4, respectivamente, del Real Decreto Legislativo 1/2016, de 16 de diciembre, por el cual se aprueba el texto refundido de la Ley de prevención y control integrados de la contaminación.

  Siempre que sea posible, la empresa contratista deberá hacer una elección inteligente de materiales (uso de materiales adecuados para el medio ambiente, evitando los que no lo sean), equipos de eficiencia energética (reducir el coste energético y la huella de carbono colectivo), final de la vida útil y reutilización, etc.

4.2 Marco de cumplimiento normativo

El actual marco normativo para las entidades públicas de Cataluña está establecido, principalmente, en la Política de Ciberseguridad de la Generalitat de Cataluña de septiembre del 2021. Esta política recoge directivas y reglamentos del Parlamento y del Consejo Europeo, Reales Decretos del estado español, así como instrucciones de la Generalitat de Cataluña. Este marco de cumplimiento normativo en temas de ciberseguridad y protección de datos, abarca a las entidades públicas de la Generalitat de Cataluña y a todos aquellos que participan en la prestación de sus servicios.

4.3 Datos de carácter personal

El adjudicatario tratará los datos de carácter personal a los que acceda como consecuencia de la ejecución de este contrato de conformidad con lo establecido en la normativa vigente en la materia.

La empresa adjudicataria se responsabilizará del uso adecuado de la información que se pueda obtener con el fin de proteger los datos personales, a lo largo de toda la fase de realización del objeto del contrato y también una vez finalizada la misma, sobre la base de las normativas internacionales al respecto que son de obligado cumplimiento, entre ellas y expresamente, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que refiere al tratamiento de datos personales y a la libre circulación de los mismos, así como cualquier otra normativa nacional y de la Unión Europea que sea aplicable en materia de protección de datos y en relación con los datos personales a los que tenga acceso durante la vigencia de este contrato.

El incumplimiento de estas obligaciones constituye la infracción tipificada en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, sin perjuicio de las responsabilidades exigidas ante la jurisdicción ordinaria.

El Adjudicatario, en relación con aquellos datos que por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) sea necesario, en la solución propuesta debe cumplirlo; por ejemplo, ubicar los datos en una base de datos física diferente, cifrar los datos, control de acceso, etc.

El Adjudicatario se compromete a cumplir, en relación con los datos tratados en la ejecución del presente contrato:

- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Las buenas prácticas para la gestión de la seguridad de la información

Firmado digitalmente por: Carme Fàbregas Casas
2026.06.02 12:30:56 +02'00'

Carme Fàbregas Casas
Directora del Área de Sistemas e innovación
Firmado electrónicamente