



Memoria Justificativa y Solicitud de Contratación

**OBJETO A CONTRATAR: CONTRATO POR LOTES PARA EL
SUMINISTRO Y DOTACIÓN DE SISTEMAS DE SEGURIDAD
INFORMÁTICA Y CIBERSEGURIDAD**

NÚMERO DE LA S.C: 2000002778

Dirección /Gerencia:	Explotación Ferroviaria Metro de Madrid, S.A.	Área:	Sistemas de Información
División:	Ingeniería y Mantenimiento	Servicio:	Explotación de Sistemas y Seguridad Informática

Aprobado por: Carlos Cuadrado

1 OBJETO DE LA SOLICITUD DE CONTRATACIÓN

El presente documento tiene por objeto elevar a la aprobación del correspondiente órgano de contratación de Metro de Madrid, S.A., la autorización para el inicio de un proceso de licitación que tiene por objeto la contratación del contrato por lotes para el suministro y dotación de sistemas de seguridad informática y ciberseguridad.

En la presente solicitud de contratación se contemplan los siguientes lotes:

- **Lote 1:** Suministro de licencias de la solución de gestión de dispositivos móviles (MDM).
- **Lote 2:** Suministro de licencias de módulos de balanceo geográfico y cortafuegos para balanceadores.
- **Lote 3:** Suministro de licencias de usuario y tokens para la conexión remota a la red corporativa.
- **Lote 4:** Suministro de licencias de antivirus / antimalware / anti APT y actualización de licencias de antivirus / antimalware.

2 DATOS DE LA LICITACIÓN

▪ Objeto

Contratación consistente en el suministro y dotación de sistemas de seguridad informática y ciberseguridad orientados a reforzar principalmente la seguridad los servicios publicados en Internet (como por ejemplo la Web corporativa o el nuevo Andén Central), los accesos remotos a la red corporativa, los ordenadores y puestos de trabajo del personal de la empresa, y los dispositivos móviles tanto corporativos como de propósito específico (de uso industrial). En algunos casos, los lotes responden a necesidades recurrentes en el tiempo, por crecimiento del número de usuarios o del parque de equipos, o bien responden a nuevas necesidades por la implantación de nuevas plataformas tecnológicas, nuevos servicios publicados en Internet u ofrecer respuesta a nuevos escenarios de riesgos en materia de Ciberseguridad. El desglose de estos sistemas es:

- **Lote 1:** Suministro de licencias de la solución de gestión de dispositivos móviles (MDM).
- **Lote 2:** Suministro de licencias de módulos de balanceo geográfico y cortafuegos para balanceadores.
- **Lote 3:** Suministro de licencias de usuario y tokens para la conexión remota a la red corporativa.
- **Lote 4:** Suministro de licencias de antivirus / antimalware / anti APT y actualización de licencias de antivirus / antimalware.

En todos y cada uno de los lotes contemplados, es condición indispensable que el suministro y dotación incluya, en los términos especificados para cada caso, los respectivos servicios de mantenimiento y soporte técnico, y la suscripción de licencias y de servicios en los que aplique, tal que se asegure la resolución de incidencias, tanto de hardware como de software, la sustitución / reemplazo en caso de averías o roturas, y el derecho de uso del software y/o de los servicios de suscripción, tal que garanticen la completa operatividad de los mismos; así como disponer de nuevas versiones, actualizaciones y parches, y acceso a bases de datos y documentación del fabricante. Igualmente, permite que los sistemas de seguridad informática se encuentren en un estado funcional óptimo.

▪ **Servicio responsable de la ejecución del contrato**

Servicio de Explotación de Sistemas y Seguridad Informática.

▪ **Valor estimado del contrato (artículo 101)**

Valor estimado: 409.000,00 euros (IVA no incluido)

▪ **Método de cálculo aplicado para determinar el valor estimado (artículo 101)**

☒ El valor real de los distintos contratos análogos adjudicados durante el ejercicio precedente, ajustado en función de los precios habituales en el mercado y de los cambios en el número de unidades de materiales a suministrar.

▪ **Presupuesto base de Licitación (Art. 100)**

- Base imponible (BI): 409.000,00 euros
- Importe del I.V.A.: 85.890,00 euros
- Presupuesto base de licitación (PBL): 494.890,00 euros, IVA incluido

Desglose por lotes:

Lote	BI (€)	IVA (€)	PBL (€)
1	134.000,00 €	28.140,00 €	162.140,00 €
2	70.000,00 €	14.700,00 €	84.700,00 €
3	112.000,00 €	23.520,00 €	135.520,00 €
4	93.000,00 €	19.530,00 €	112.530,00 €

▪ **Desglose del presupuesto base de licitación (Art. 100.2)**

- Costes Directos: 494.890,00 euros, (IVA incluido)
- Costes Indirectos: 0 euros, (IVA incluido)
- Otros eventuales gastos: 0 euros, (IVA incluido)

▪ **Modificación del contrato**

☒ No procede

☐ Procede

▪ **División en lotes:**

☒ **Sí se divide en lotes (Art. 99.4)**

- Número de lotes: 4

- Objeto de cada lote:

- **Lote 1:** Suministro de licencias de la solución de gestión de dispositivos móviles (MDM).
- **Lote 2:** Suministro de licencias de módulos de balanceo geográfico y cortafuegos para balanceadores.
- **Lote 3:** Suministro de licencias de usuario y tokens para la conexión remota a la red corporativa.
- **Lote 4:** Suministro de licencias de antivirus / antimalware / anti APT y actualización de licencias de antivirus / antimalware.

Limitación en la presentación de ofertas

- Los licitadores podrán presentar oferta a los lotes que deseen:

☒ Sí

☐ NO

Limitación en el número de lotes que pueden adjudicarse a cada licitador

- Los licitadores sólo podrán ser adjudicatarios de un número limitado de lotes:

☒ NO

☐ Sí

☐ NO se divide en lotes (Art. 99.3)

■ **Duración del contrato**

- Plazo de duración/ejecución inicial del contrato:
 - **Lote 1:** Veintiún (21) meses, de acuerdo con lo expresado a continuación:

Un (1) mes para el suministro desde el día siguiente a la fecha de formalización del contrato.

Veinte (20) meses para el soporte y mantenimiento desde el suministro.
 - **Lote 2:** Trece (13) meses, de acuerdo con lo expresado a continuación:

Un (1) mes para el suministro desde el día siguiente a la fecha de formalización del contrato.

Doce (12) meses para el soporte y mantenimiento desde el suministro.
 - **Lote 3:** Dieciocho (18) meses, de acuerdo con lo expresado a continuación:

Un (1) mes para el suministro desde el día siguiente a la fecha de formalización del contrato.

Diecisiete (17) meses para el soporte y mantenimiento desde el suministro.
 - **Lote 4:** Veintinueve (29) meses, de acuerdo con lo expresado a continuación:

Seis (6) meses para el suministro desde el día siguiente a la fecha de formalización del contrato.

Veintitrés (23) meses para el soporte y mantenimiento desde el suministro.
- Hito a partir del cual comienza la duración/ejecución del contrato:
 - ☒ A partir del día siguiente a la formalización del contrato
 - ☐ A partir del día siguiente a la firma del acta de replanteo
 - ☐ A partir del día siguiente a la firma del acta de inicio de los trabajosPrórrogas:
 - ☒ NO
 - ☐ Sí

■ **Clasificación del contrato**

- ☒ Sujeto a LCSP (Ley 9/2017)
- ☐ Sujeto a LCSE (Ley 31/2007)

▪ **Naturaleza del contrato**

- ☐ Servicios
- ☒ Suministros
- ☐ Obras
- ☐ Mixto (servicios/suministros/obras)

▪ **Procedimiento de licitación**

- ☒ Procedimiento Abierto
- ☐ Procedimiento Abierto Simplificado
- ☐ Procedimiento Abierto Súper-Simplificado
- ☐ Procedimiento con negociación y concurrencia
- ☐ Procedimiento negociado sin publicidad y sin concurrencia (contratista único)

▪ **Criterio de adjudicación (Arts. 145 y 146)**

- ☐ Pluralidad de criterios en base a la mejor relación **calidad-precio**
- ☐ Pluralidad de criterios en base a la mejor relación coste-eficacia (sobre la base del precio o coste)
- ☒ Único criterio (precio o criterio basado en rentabilidad)

Justificar las razones por el que se propone este criterio de adjudicación: Los productos a adquirir están perfectamente definidos - técnica y económicamente - por cada uno de los fabricantes no siendo posible introducir modificaciones de ninguna clase respecto de sus funcionalidades, prestaciones y/o características técnicas. Igualmente, el soporte y mantenimiento de los productos se prestan en las condiciones técnicas y económicas establecidas por el fabricante bien sea de forma directa o a través del canal de empresas certificadas o acreditadas¹.

En consecuencia, no es posible que los oferentes presenten propuestas con variaciones ni en los productos ni en sus condiciones de soporte y mantenimiento, ni es susceptible de introducirse ninguna modificación en el contrato. Las propuestas de los oferentes solo podrían diferenciarse en el precio ofertado.

¹ Es el fabricante quien establece niveles de soporte, canales de comunicación y atención, condiciones de uso del software y el hardware, etc.

▪ **Subcontratación**

☐ No procede

☒ Procede.

Indicar las tareas críticas que no podrán ser objeto de subcontratación: Ninguna.

▪ **Procedimiento de subasta electrónica o petición sucesiva de ofertas**

☒ NO

☐ SI

▪ **Fondos FEDER**

☒ Contrato no financiable con fondos FEDER

☐ Contrato financiable con fondos FEDER

▪ **Confidencialidad de los Pliegos de Prescripciones Técnicas**

☐ NO

☒ SI

☒ En su totalidad

☐ En parte del contenido

El Pliego de Prescripciones Técnicas² de la licitación incluye detalles técnicos y características de algunos de los sistemas de seguridad informática y ciberseguridad implementados en Metro de Madrid que, en muchos casos, también se utilizan para la protección de los servicios informáticos y las plataformas tecnológicas en que se soportan algunos de los servicios esenciales e infraestructuras críticas de la empresa.

Su divulgación pública podría llegar a suponer que terceros ajenos a la empresa, incluso con intereses ilegítimos o malintencionados, dispongan de información relevante para planificar y perpetrar un ataque informático que suponga una afectación para Metro de Madrid.

3 ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

A continuación, se incluye la justificación de la necesidad de acometer cada una de las contrataciones propuestas, así como reflejar los contratos precedentes que puedan

² En cuanto al Pliego de Condiciones Particulares, se considera que puede publicarse en tanto se ha evitado dar detalles técnicos (esencialmente denominaciones y características de productos y nombres de fabricantes, incluso en las denominaciones de los lotes) que pueden utilizarse para los fines indicados en relación con la información contenida en el Pliego de Prescripciones Técnicas.

estar relacionados con cada una de las acciones y comparativa de los alcances de los contratos precedentes en los casos en que aplique. La información se agrupa por cada uno de los lotes propuestos destacando que se ha intentado agrupar lo más posible en función de las características y similitudes de los elementos a incluir en cada uno de los lotes.

3.1 Lote 1: Suministro de licencias de la solución de gestión de dispositivos móviles (MDM)

El objeto de la acción es contratar el suministro de licencias de la solución de gestión de dispositivos móviles (MDM) basada en tecnología WorkSpace ONE del fabricante VMWare³.

Los dispositivos móviles han proliferado en el entorno profesional a un ritmo muy elevado, no siendo menos en el caso de Metro. El creciente número de modelos de dispositivos, plataformas y versiones de sistema operativo disponibles, suponen nuevos y complejos retos de administración y gestión del parque de dispositivos móviles corporativos, así como, de la seguridad de la información empresarial a la que se accede desde los mismos.

³ La empresa AirWatch, creador de la tecnología, ha sido adquirida por VMWare; tras lo cual, el producto ha pasado a denominarse WorkSpace ONE produciéndose también un cambio en el modelo de licenciamiento.

Metro, dispone de un gran número de dispositivos móviles que acceden a servicios corporativos, facilitando enormemente el trabajo, como son los siguientes: 1) el terminal del Supervisor Comercial de Bajo Coste (SCBC), impulsado por el Área de Ingeniería para la gestión de las estaciones; 2) los terminales de ENRUTA y SUMATE, impulsados por el Servicio de Logística del Área de Aprovisionamiento para la gestión de las rutas de recogida y reparto de mensajería y materiales, y la gestión del suministro de materiales a las estaciones respectivamente; 3) el terminal de inspección, impulsado por el Servicio de Proyectos y Soporte Operativo del Área de Gestión Operativa para la realización de las inspecciones a viajeros en la red, 4) los terminales para proporcionar información en las obras de mejora de las diferentes líneas a lo largo de 2017 y 2018, impulsado por el Área de Gestión Operativa y el Servicio de Canales Digitales, y 5) los terminales corporativos con acceso a aplicaciones y sistemas informáticos como el correo electrónico, Netro, Incimov Mobile o Icaro.

En este sentido, cada una de las líneas de servicios indicados conllevan un crecimiento en el tiempo derivado de la incorporación de nuevos dispositivos móviles en cada ámbito, Pero, más allá de este crecimiento, existen proyectos en marcha, y pilotos que se traducirán en proyectos, que suponen el despliegue y puesta en funcionamiento de mayor número de dispositivos móviles, destacando: 1) el terminal, o Tablet, para la gestión en las estaciones, impulsado por el Servicio de Gestión Operativa de Líneas, que supondrán un total de 587 dispositivos (incluyendo los ya existentes), 2) el terminal para la movilidad de los grupos de mantenimiento, o TPL 2.0, impulsado por los Servicios de Ingeniería de Mantenimiento de Instalaciones y Comunicaciones y de Mantenimiento de Electrificación, Señales y Comunicaciones respectivamente, que supondrá inicialmente 512 dispositivos (pudiéndose incrementar hasta un total de 685) y 3) el terminal para la movilidad de la sección de conservación de mantenimiento de ciclo corto, impulsado por el Área de Mantenimiento de Material Móvil, que supondrá un total de 15 dispositivos para realizar el piloto.

Para dar solución orientada a una administración y gestión eficiente de los dispositivos, sin que tenga que ser manual y presencial con los costes que ello supone, así como, ofrecer un acceso seguro a la información corporativa desde los mismos y/o disponer de la capacidad de actuar en el caso de pérdida o robo del dispositivo para evitar fugas de información, se dispone de una Plataforma de Gestión de Dispositivos Móviles (MDM), basada en tecnología Workspace ONE del fabricante VMWare para centralizar la gestión de los dispositivos de forma simple, eficiente y remota, de la que se dispone 470 licencias para gestionar igual número de dispositivos acorde a las necesidades actuales.

En relación con las licencias, cabe destacar que, tras la adquisición de la empresa AirWatch⁴ por parte de VMWare, ha variado la denominación del software – en la actualidad Workspace ONE, el modelo de licenciamiento – ahora standard, advanced y enterprise edition⁵ –, las funcionalidades incluidas en cada tipo de licencia, y el precio de lista. Es la versión advanced la que incluyen las funcionalidades indispensables en Metro de Madrid como son: el control remoto avanzado (Advanced Remote Control), el contenedor seguro de información (Content Locker), el correo electrónico seguro (Boxer), el navegador seguro (Browser), la implementación de túneles seguro por aplicación, y la gestión de la identidad, así como la posibilidad de gestionar dispositivos con Windows 10 además de basados en IOS o Android.

En este sentido, de las 470 licencias adquiridas por Metro de Madrid: 195 son del tipo Green management y 275 del tipo Rugged que equivalen a los tipos standard y advanced en el nuevo modelo. Por lo tanto, además de adquirir las licencias necesarias para atender las necesidades de gestión de los dispositivos que se integrarán tras la puesta en marcha de los proyectos mencionados, y que se cifran en 950 licencias del tipo advanced edition, es también necesario realizar una actualización de las 195 licencias del tipo Green management al tipo advanced edition.

El objeto de la presente acción es el suministro de las licencias del software de gestión de dispositivos móviles para cubrir las necesidades indicadas. Según evolucione su utilización y en función del volumen de la plataforma gestionada, se planteará a futuro el reforzarla y aumentar sus capacidades.

En el caso de no acometer la acción, no se podrían abordar los proyectos mencionados, ni gestionar y ofrecer seguridad a los dispositivos con las garantías exigidas por Metro de Madrid.

El suministro de licencias para la solución de gestión de dispositivos móviles (MDM) tiene asociados contratos ejecutados anteriormente, a saber:

Empresa	Contrato nº	Período	Importe Contrato	Licencias	Importe por Licencia
Navarra Tecnología del Software, S.L.	7714000260	Agosto 2014	6.810,00 €	150	36,60 € ⁶
Navarra Tecnología del Software, S.L.	7715000121	Mayo 2015	732,00 €	20	36,60 €
Servicios Microinformática, S.A.	7717000232	Julio 2017	12.009,00 €	300	40,03 €

Nota: Los contratos nº 7714000260 y 7715000121 corresponden a licencias del tipo Green Management y el contrato nº 7717000232 corresponde a 25 licencias del tipo Green Management y 275 del tipo Rugged. En todos los casos, las licencias se adquieren en modalidad perpetua con un (1) año de soporte y mantenimiento que debe renovarse anualmente.

⁴ Empresa creadora y desarrolladora de la tecnología.

⁵ En el modelo de licenciamiento de AirWatch existían los tipos: Green management, blue management, orange management y rugged.

⁶ El coste unitario por licencia (incluyendo soporte y mantenimiento anual) es de 36,60 € para un total de 150 licencias adquiridas. Adicionalmente, el importe del contrato incluía 1.320,00 € de servicios de instalación y configuración.

3.2 Lote 2: Suministro de licencias de módulos de balanceo geográfico y cortafuegos para balanceadores

El objeto de la acción es contratar el suministro de licencias de los módulos de balanceo geográfico (DNS) y de cortafuegos (AFM) respectivamente, bajo la modalidad Better Bundle según denominación del fabricante, para las dos parejas de equipos F5 modelo 4200v que se utilizan para el balanceo de servicios en la red interna y que se ubican respectivamente en el CTI de Campo de las Naciones y en el CCS de Canillejas.

Desde el Área de Sistemas de Información (ASI), a través del Servicio de Explotación de Sistemas y Seguridad Informática, se implanta y mantiene una gran cantidad de servicios informáticos corporativos, desarrollados y/o soportados en tecnologías variadas, y que operan las 24 horas, los 7 días de la semana, los 365 días del año, requieren de una infraestructura tecnológica específica que garantice la seguridad, la disponibilidad y el rendimiento de los servicios informáticos corporativos publicados tanto interna como externamente.

Dicha infraestructura tecnológica está constituida por equipos de balanceo que se encargan, por un lado, de realizar un reparto de la carga de trabajo entre los diferentes servidores de aplicación, proporcionando mayor eficiencia y garantizando la disponibilidad de la aplicación ante fallos eventuales y, por otro lado, de optimizar los tiempos de respuesta y asegurar el acceso a las aplicaciones, descargando a los servidores de dichas funciones e, incluso, redirigiendo las peticiones a los servidores activos en el caso de avería o paradas de mantenimiento de éstos.

Por otro lado, y mucho más importante aún, añaden una capa de seguridad para evitar ataques informáticos contra los diferentes sistemas dada la exposición a una amplia variedad de ataques maliciosos. Además ofrecen un balanceo geográfico entre los diferentes Centros de Proceso de Datos de Metro, opción especialmente útil en situaciones de contingencia. Así pues, los balanceadores son equipos hoy en día imprescindibles para poder dar una mínima garantía razonable de disponibilidad de los servicios informáticos corporativos pero requieren la integración de diferentes módulos software para proporcionar todas estas funcionalidades.

En este caso concreto, se requiere que los balanceadores relativos a los servicios publicados internamente (entre los que cabe destacar el pago electrónico, los módulos HSM para el servicio de venta, los sistemas de gestión empresarial, el correo electrónico, SAP, GDL, Andén Central, Portafirma, Autofirma, etc.) dispongan de:

- El modulo DNS que se usa principalmente para hacer balanceo geográfico de servicios en este caso entre los Centro de Procesos de Datos en que se ubican los servidores de aplicaciones: Centro de Tecnologías de la Información – CTI – sito en Campo de las Naciones y el Centro de Continuidad del Servicio – CCS – sito en Canillejas. Así, el balanceador actúa como servidor DNS (resolución de nombres de máquinas o servicios) devolviendo al cliente la dirección IP donde el servicio se presta de la forma más óptima según la configuración de balanceo realizada. De esta forma por cada servicio se pueden tener recursos en

diferentes centros facilitando la prestación del servicio por ejemplo cuando exista una incidencia o contingencia en uno de ellos, y sin afectar al usuario.

- El módulo AFM es un cortafuegos firewall, de nivel 4, que proporciona seguridad a nivel de las comunicaciones relativas a los servicios publicados mitigando o reduciendo el nivel de exposición a una amplia variedad de ataques maliciosos y que, principalmente, permite la actuación proactiva para prever situaciones de riesgo, en lugar de tener que hacerlo de forma reactiva una vez identificado un patrón de ataque.

El objeto de la presente acción es el suministro de licencias de los módulos de balanceo geográfico (DNS) y de cortafuegos (AFM) para balanceadores F5 modelo 4200v para cubrir las necesidades indicadas dotando a los balanceadores de mayores funcionalidades.

En el caso de no acometer la acción, no se podría realizar balanceo geográfico entre los recursos informáticos de los servicios / sistemas / aplicaciones existentes en diferentes centros de procesamiento de datos, penalizando la disponibilidad de dichos servicios para los usuarios, ni se incrementaría la seguridad de la información y de los servicios afectando de forma directa a proyectos clave como la puesta en producción del nueva Andén Central o los sistemas de Portafirma y Autofirma.

El suministro de licencias de módulos de balanceo geográfico (DNS) y de cortafuegos (AFM) para balanceadores F5 modelo 4200v no tiene contratos iguales o similares que se hayan ejecutado con anterioridad; por lo tanto, no es posible realizar una comparativa económica.

3.3 Lote 3: Suministro de licencias de usuario y tokens para la conexión remota a la red corporativa

El objeto de la acción es contratar el suministro tanto de licencias de usuario del software RSA Authentication Manager como de tokens – hardware y software – de RSA para la conexión remota a la red corporativa de Metro de Madrid.

El Área de Sistemas de Información (ASI), ofrece a los usuarios de la red corporativa, tanto personal de la organización como de las empresas colaboradoras, la posibilidad de acceder remotamente en modo seguro a los servicios informáticos de la empresa.

Este acceso puede ser llevado a cabo desde redes externas, privadas o públicas, mediante una conexión VPN (red privada virtual), que utiliza un sistema de autenticación fuerte de doble factor, mediante la combinación de un PIN (o clave), con una contraseñas de un solo uso (o passcode) generada de forma aleatoria y no predecible para proveer el acceso de los usuarios.

Es necesario un mecanismo de acceso de doble factor de autenticación (el cual, se explicará más adelante), debido a que se puede acceder a Metro de Madrid desde equipos ajenos a la empresa y de los que no se puede asegurar su estado, respecto a si tienen antivirus actualizado, anti spyware y otras medidas mínimas de seguridad. No

hacerlo supondría un grave riesgo de seguridad, dado que si uno de esos equipos fuera interceptado por un hacker, sería trivial acceder a los sistemas de Metro.

Es por ello, que se propone no solo continuar utilizando, sino extender en los casos que sea necesario, el uso de un sistema de autenticación de doble factor que permite evitar ataques (por ejemplo, de fuerza bruta, de diccionarios y/o de secuestro de sesiones activas), que podría utilizar un atacante para acceder a la red de Metro de Madrid con fines malintencionados. Este sistema se basa en que para acceder, no solo se necesita conocer un dato (usuario o/y parte de la contraseña), sino disponer de un dispositivo que propone otra contraseña cambiante con el tiempo y dependiente del usuario que se denomina token (pudiendo ser de tipo hardware o software).

Este servicio hace posible extender la infraestructura de red corporativa, favoreciendo la movilidad de los agentes, ganando en tiempo de reacción ante eventos que requieran la conexión a la red, y ofreciendo la disponibilidad de la información necesaria en cualquier momento y lugar. Es imprescindible para que los usuarios se puedan conectar de forma segura a la red corporativa, siendo especialmente destacable el caso del personal directivo que debe estar siempre disponible ante necesidades de la empresa, o personal técnico que requiere conectarse para atender incidencias, disminuyendo el tiempo de resolución al no ser necesario desplazarse a las instalaciones de la empresa. También, se utiliza para el acceso de personal de empresas colaboradoras, que podrían trabajar en remoto de forma segura sin suponer un coste adicional para Metro de Madrid por necesidad de un puesto físico.

Igualmente, disponer de este tipo de sistemas de autenticación es también indispensable para cumplir con disposiciones legales, entre las que cabe destacar la legislación, tanto europea como española, en materia de protección de datos de carácter personal y de protección de infraestructuras críticas.

En la actualidad, se tiene la capacidad para ofrecer el servicio a un total de 775 usuarios⁷, lo que se traduce en igual número de licencias del producto RSA Authentication Manager Base Edition v8.3 SP2, así como tokens – hardware y software⁸ – suficientes para atender las renovaciones y nuevas asignaciones para 2018. Sin embargo, se prevé que el número de usuarios se incremente al llevarse a cabo la integración de las varias conexiones VPN existentes (que se cifra en 225 licencias); lo cual, supone también un incremento en cuanto a las necesidades de token más allá de las derivadas de las renovaciones o los crecimientos vegetativos, que conlleva la necesidad de adquirir 450 token hardware y 950 token software para un horizonte temporal de tres (3) años.

El objeto de la presente acción es el suministro de licencias de usuario del software RSA Authentication Manager y de tokens - hardware y software - para la conexión remota a la red corporativa para cubrir las necesidades indicadas. Según evolucione su utilización y en función del volumen de crecimiento de usuarios, se planteará a futuro el reforzarla y aumentar sus capacidades.

⁷ El número de licencias se ha mantenido estable en los últimos años – desde 2011 - en tanto la última adquisición se hizo con previsión de futuro.

⁸ En la actualidad los token software se destinan para los usuarios internos tal que se le pueda instalar en el ordenador y/o en el teléfono móvil; mientras que, los modelos hardware se destinan principalmente a empresas colaboradoras externas.

En el caso de no acometer la acción, no se podría proporcionar un mecanismo de acceso seguro a la red corporativa de Metro de Madrid desde redes externas - públicas y privadas - todo ello con las garantías de seguridad requeridas y en consonancia con los requisitos legales y normativos.

El suministro de licencias y de token para el acceso remoto seguro a la red corporativa tiene asociados contratos ejecutados anteriormente y que, en parte o totalmente, son equiparables:

- En cuanto a la adquisición de licencias:

Empresa	Contrato nº	Período	Importe Contrato	Licencias	Importe por Licencia
Sistemas Avanzados de Tecnología, S.A. (SATEC)	4809000013	Abril 2009	4.047,00 €	50	80,94 €
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7709000362	Nov. 2009	3.389,50 €	50	67,79 €
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7710000117	Mayo 2010	11.020,50 €	150	73,47 €
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7710000537	Dic. 2010	10.563,52 € ⁹	75	67,17 €

Nota: Se han reflejado todos y cada uno de los contratos de adquisición y ampliación de licencias a partir de la implantación inicial del sistema que se dimensionó para 500 usuarios en ese momento.

- En cuanto a la adquisición de token:

Empresa	Contrato N°	Período	Importe Contrato	Importe Unitario (x Dispositivo para 60 meses)	Importe Unitario (x Dispositivo para 36 meses)	Importe Unitario (x Dispositivo para 24 meses)	Importe Unitario Equivalente Anual	Diferencia Respecto Contrato Anterior
Sistemas Avanzados de Tecnología, S.A. (SATEC)	4809000122	Ag. 2009	6.390,31 €	63,90 €			12,78 €	n/a
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7710000156	Jun. 2010	9.187,50 €	61,25 €			12,25 €	-4,15 %
Informática El Corte Inglés, S.A. (IECISA)	7710000444	Oct. 2010	10.252,03 €	68,34 €			13,67 €	11,58 %
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7710000537	Dic. 2010	10.563,52 € ¹⁰	61,39 € token HW 49,12 € token SW			12,28 € token HW 9,82 € token SW	-10,17 % token HW n/a token SW

⁹ El importe equivalente es 5.037,75 €; ya que, el resto se destinó a la adquisición de token de RSA.

¹⁰ El importe equivalente es 5.525,77 €; ya que, el resto se destinó a la adquisición de licencias de RSA Authentication Manager para proveer acceso a mayor número de usuarios.

Vintegris, S.L.	7714000462	Dic. 2014	7.797,60 €	--	33,93 € token HW 27,09 € token SW		11,31 € token HW 9,03 € token SW	-7,88 % token HW -8,08 % token SW
ATOS Spain, S.A.	7715000224	Jul. 2015	12.815,79 €			34,20 € token HW 25,56 € token SW	17,10 € token HW 12,78 € token SW	51,19 % token HW 41,53 % token SW
Grupo Seidor, S.A.	7717000065	Marzo 2017	11.878,36 €			39,34 € token HW 26,74 token SW	19,67 € token HW 13,37 € token SW	15,02 % token HW 4,62 % token SW
BT España, S.A.U	7718000038	Feb. 2018	16.324,11 €			38,30 € token HW 21,59 token SW	19,15 € token HW 10,80 € token SW	-2,65 % token HW -19,25 % token SW

3.4 Lote 4: Suministro de licencias de antivirus / antimalware / anti APT y actualización de licencias de antivirus / antimalware

El objeto de la acción es contratar el suministro de licencias del software antivirus, antimalware y anti APT (amenazas avanzadas persistentes o malware avanzado), así como la actualización del tipo de licencia del software antivirus / antimalware para los puestos cliente.

El Área de Sistemas de Información ofrece servicios informáticos esenciales a los usuarios de la red corporativa, incluyendo, tanto personal interno, como de las empresas colaboradoras. El acceso a los servicios informáticos se realiza desde ordenadores en los cuales se tiene desplegado el software antivirus / antimalware McAfee Endpoint Threat Protection (ETP), al que se integra el software McAfee Threat Intelligence Exchange (TIE) orientado a evitar el malware avanzado conocido como APT (amenazas avanzadas persistentes), ambos gestionados a través de una consola común denominada ePO, y todos ellos del fabricante McAfee. Además de los equipos ofimáticos (ordenadores de sobremesa y portátiles), también, se ofrece protección a los servidores.

La combinación de estas soluciones sirve para proveer una protección dinámica contra virus, malware, malware avanzado o dirigido y amenazas similares que pueden ser detectadas y neutralizadas con este mecanismo; además de ofrecer una prevención adaptable contra las amenazas a partir de la compartición de los datos de seguridad entre los diferentes elementos a securizar y fuentes externas, posibilitando una respuesta común y temprana ante lo que pueda identificarse como una tendencia o comportamiento que pueda constituir un ataque.

Es importante destacar que la aparición de nuevos escenarios de riesgo (en gran medida orientados a la ejecución de ataques dirigidos y persistentes en el tiempo), hacen que se deba responder eficaz y eficientemente, requiriéndose una protección adaptable orientada a reducir el intervalo entre la detección y la contención de los

ataques más tradicionales basados en virus, malware y cualquier otro tipo de programa malicioso que con el uso de herramientas más tradicionales.

En dicho contexto las soluciones McAfee Endpoint Threat Protection y McAfee Threat Intelligence Exchange (TIE) se encargan de detectar situaciones de riesgo por virus / malware en los equipos ofimáticos (y servidores), evitando que se produzca el efecto buscado por el software malicioso destacando que, en los dos últimos años han sido de vital importancia para detectar y neutralizar los ataques mediante el malware, denominado “ransomware”¹¹, escenario que ha requerido implementar reglas concretas de detección y contención de los ataques en el software antivirus, y principalmente poder actuar de forma proactiva.

Por otro lado, más allá de períodos de fin de vida y/o de soporte y mantenimiento de los diferentes productos, el fabricante McAfee ha ido evolucionando las suites de productos antivirus / antimalware, entre otras razones, para incorporar nuevas funcionalidades y para adaptarse a la evolución de los sistemas operativos de los equipos ofimáticos, destacando el caso de Windows 10 para equipos de uso individual. En este sentido, la suite Endpoint Threat Protection (ETP) ha evolucionado a la denominada Complete Endpoint Protection (CTP) que incluye nuevas funcionalidades como son: Dynamic Application Containment (DAC) orientada a evitar la ejecución de aplicaciones de reputación desconocida que podrían realizar actividades maliciosa y Real Protect – Machine Learning orientada a detectar malware del tipo día cero, es decir, aquellos que aún no se han hecho público, realizado mediante una combinación de análisis estático (pre-ejecución) y dinámico (post-ejecución).

El objeto de la presente acción es, por un lado, el suministro de trescientas (300) nuevas licencias de McAfee Complete Endpoint Protection (CTP) y de McAfee Threat Intelligence Exchange (TIE) respectivamente, que se añadirán a las 3.200 licencias existentes, para dar cobertura al crecimiento de nuevos equipos (ordenadores portátiles y sobremesa, y servidores) ofreciendo seguridad a los mismos. Y, por otro lado, la actualización de las 3.200 licencias de McAfee Endpoint Threat Protection (ETP) a la suite McAfee Complete Endpoint Protection (CTP) para asegurar la continuidad del producto en el tiempo, ofrecer una solución más adecuada a la evolución del sistema operativo principalmente de los equipos cliente (portátiles y sobremesa) y aprovechar las nuevas funcionalidades para ofrecer una seguridad mucho más eficiente y proactiva.

En el caso de no acometer la acción, no se podría proporcionar un mecanismo de seguridad a los nuevos ordenadores y servidores que se implementen en la plataforma informática de Metro de Madrid, ni evolucionar la solución para ofrecer una seguridad eficiente y proactiva principalmente ante situaciones de malware avanzado, persistente y dirigido, que ha crecido en los últimos años.

El suministro de licencias del software antivirus, antimalware y anti APT tiene asociados contratos ejecutados anteriormente y que, en parte o totalmente, son equiparables:

¹¹ Del que el conocido como Cryptolocker es la variante más conocida.

- En cuanto a la adquisición de licencias del software ETP:

Empresa	Contrato nº	Período	Importe Contrato	Licencias	Importe por Licencia
Bechtle Direct, S.L.U.	7716000016	Febrero 2016	5.833,10 €	641	9,10 €

Nota: Las 2.559 licencias no reflejadas en el cuadro fueron adquiridas en el marco de los contratos de externalización del servicio de gestión, administración y soporte y mantenimiento de la plataforma microinformática de Metro de Madrid. Dichas licencias se iban adquiriendo en virtud de las necesidades detectadas, siempre siendo el titular Metro de Madrid, y se consolidaban en el inventario de software hasta llegar a la cantidad indicada.

- En cuanto a la adquisición de licencias del software TIE:

Empresa	Contrato nº	Período	Importe Contrato	Licencias	Importe por Licencia
Bechtle Direct, S.L.U.	7715000282	Octubre 2015	19.550,18 € ¹²	2.559	3,42 €
BT España	7717000132	Mayo 2017	3.704,98 €	641	5,78 €

4 INFORMACIÓN PRESUPUESTARIA

PRESUPUESTO DE INVERSIÓN

La información presupuestaria se organiza por cada uno de los lotes contemplados en la siguiente solicitud de contratación:

- **Lote 1:**

AÑO	2019
IMPORTE PERMITIDO	134.000,00 €
PEP	N2033
EXPEDIENTE	08.058

- **Lote 2:**

AÑO	2019
IMPORTE PERMITIDO	70.000,00 €
PEP	N2484
EXPEDIENTE	08.058

- **Lote 3:**

¹² El importe equivalente es 8.751,78 €; ya que, el resto se destinó a la implantación del software y su certificación por parte del fabricante.

AÑO	2019
IMPORTE PERMITIDO	112.000,00 €
PEP	N1385
EXPEDIENTE	08.058

- **Lote 4:**

AÑO	2019
IMPORTE PERMITIDO	93.000,00 €
PEP	N2033
EXPEDIENTE	08.058