PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HAN DE REGIR LOS SERVICIOS DE "MANTENIMIENTO (RENOVACIÓN DE LICENCIAS) Y SOPORTE DE FABRICANTE) DE LOS PRODUCTOS Y EQUIPOS DE SEGURIDAD DEL FABRICANTE McAFEE PROPIEDAD DE LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS - EXPTE-Nº 16/2018"

1. *OBJETO*

El objeto del contrato es:

- Mantenimiento y soporte de **20.000** licencias del producto McAFEE **"MFE Endpoint Protection Suite 1Yr GL (P+)" (**MFE Comp EP Threat Prot UPGD P:1), destinadas a equipos informáticos (estaciones y servidores) ubicados en los centros de trabajo y Centros de Proceso de Datos (en adelante CPDs) de la Administración del Principado de Asturias (en adelante APA). 12.000 de estas licencias corresponderían al entorno sanitario.

- Mantenimiento y soporte de **12.000** licencias del producto McAFEE "**MFE Content Security Suite1:1 BZ**", destinadas a equipos de seguridad (appliances de filtrado de correo y filtrado web) ubicados en el CPD principal de la APA. Este parque de licencias alcanzará a proteger **12.000** usuarios durante un periodo de un año a contar desde la firma del contrato.

- Mantenimiento y soporte de licencias del producto McAFEE "**MFE EndPnt ProtAdv 1:1GL 10000 node Bndl**", destinadas a equipos informáticos ubicados en los centros educativos de control público. Se trata de una licencia que alcanzará a proteger **10.000** usuarios durante un periodo de un año a contar desde la firma del contrato.

- Mantenimiento y soporte de **1** licencia del producto McAFEE "MFE Network Sec Starter Mngr", destinada al equipo de IPS ubicado en el CPD principal de la APA.

- Mantenimiento (soporte de fabricante) para los siguientes equipos McAFEE, durante el periodo de un año:

  - Appliance de filtrado web "Web Gateway 5500" con S/N H040250157
    - MFE Web Gateway 5500 Appl-B (1 unidad)
  - Appliance de filtrado web "Web Gateway 5500" con S/N H040251116
    - MFE Web Gateway 5500 Appl-B (1 unidad)
  - Appliance de filtrado de e-mail "E-mail Gateway 5500" con S/N H0A1447124
    - MFE Email Gateway 5500 Appl-D (1 unidad)
  - Appliance de filtrado de e-mail "E-mail Gateway 5500" con S/N H0A1447128
    - MFE Email Gateway 5500 Appl-D (1 unidad)
  - Appliance IPS "Intrushield Global" con S/N S021252039
    - MFE Net Sec M-6050 Standard HW (1 unidad)

- MFE MM8000/6050 62.5m FailOpn Kt (4 unidades)
- MFE NetSec Redundt PwrSupply 6050 (1 unidad)
- MFE NetSec XFPGbic 850nm 8K/6050 (8 unidades)

La siguiente tabla resume los conceptos objeto del contrato:

Renovación IPS

Concepto	SKU	Descripción	Tipo	Unidades
Appliance IPS	IYVM65KADMAG	MFE Net Sec M-6050 Standard HW	Hardware	1
Appliance IPS	IMTYCM-AD-AG	MFE Network Sec Starter Mngr	Software	1
Appliance IPS	RBMM62KT1AG	MFE MM8000/6050 62.5m FailOpn Kt	Hardware	4
Appliance IPS	RBRPMSPS2AG	MFE NetSec Redundt PwrSupply 6050	Hardware	1
Appliance IPS	RBX850CG1AG	MFE NetSec XFPGbic 850nm 8K/6050	Hardware	8

Renovación WEB y EMAIL

Concepto	SKU	Descripción	Tipo	Unidades
Appliance filtrado email	EMG5500DNBDG	MFE Email Gateway 5500 Appl-D	Hardware	2
Appliance filtrado web	WBG5500BNBDG	MFE Web Gateway 5500 Appl-B	Hardware	2
Licencia usuario appliances	CSSECE-AA-JG	MFE Content Security Suite1:1 BZ	Software	12.000

RENOVACIÓN ANTIVIRUS TRADICIONAL A PROTECCIÓN AVANZADA DE ESTACIONES Y SERVIDORES

Concepto	SKU	Descripción	Tipo	Unidades
Licencia usuario AV	CTPCDE-DT-IG	MFE Comp EP Threat Prot UPGD P:1	Software	20.000

RENOVACIÓN ANTIVIRUS EDUCACIÓN

Concepto	SKU	Descripción	Tipo	Unidades
Licencia usuario AV	EPA00E10KPAL	MFE EndPnt ProtAdv 1:1GL 10000 node Bndl	Software	1

2. *CARACTERÍSTICAS DE LOS SISTEMAS ANTIVIRUS Y DE SEGURIDAD Y JUSTIFICACIÓN DE SU USO*

La realidad de uso de los equipos y redes informáticas a día de hoy marca la necesidad de una defensa plenamente actualizada atenta a detectar y abortar los intentos de ataques producidos por virus y malware en general. Se trata de ataques

cada vez más potentes y dirigidos, sumamente dañinos en cuanto que afectan a la integridad de equipos, de los archivos que contienen, así como a la fiabilidad, buen uso de las redes y accesos a internet.

Estos sistemas de defensa obligan a la implantación de antivirus para los puestos clientes en los centros de trabajo de la APA, así como en los servidores implantados en el CPD de la APA.

El sistema propuesto se basa en la continuidad y evolución de los productos Mcafee actualmente instalados que se adaptan bien a la topología implantada a día de hoy (topología que posiblemente sufra cambios que obliguen a pliegos que identifiquen la mejor solución técnica para esos sistemas cambiantes).

El McAfee Endpoint Protection facilita un sistema centralizado, mediante una plataforma de gestión conocida como consola EPO, que sin requerir consumos de recursos notables, es eficaz frente ataques de "día-cero", virus espías, troyanos, gusanos y el resto de amenazas usuales; todo ello con procesos de supervisión y auditorías válidos para las necesidades de control técnico que adquiere la Dirección General de Tecnologías de la Información y las Comunicaciones (en adelante DGTIC).

El IPS (Sistema de prevención de intrusiones) consigue dotar a la infraestructura de un nivel de seguridad adicional, protegiendo tanto a servicios como a usuarios de la organización, de ataques zero-day, malware, botnets, denegaciones de servicio y demás, ofreciendo además un nuevo punto de control sobre el tráfico de red de la organización, generando información proactiva sobre posibles amenazas en tiempo real, así como análisis de comportamiento basados en umbrales.

Así mismo, la necesidad de proteger tanto las plataformas y los envíos de correo electrónico de la APA frente a las amenazas de seguridad y el correo basura (spam), como de garantizar el acceso seguro de los usuarios de la APA a recursos y páginas de internet, y filtrar los accesos a páginas de contenido ilegal o inapropiado, todo ello de acuerdo a la política de seguridad de la información de la APA, obliga a mantener las plataformas de filtrado de correo electrónico y filtrado web implantadas, por medio de la renovación de las licencias de uso por usuario cargadas en estas plataformas.

3. *REQUISITOS DE SERVICIO*

La renovación de las licencias indicadas en el presente pliego debe incluir los servicios asociados a dicha renovación, tales como el acceso a nuevas versiones de software o resolución de incidencias y consultas relativas al funcionamiento de las mismas, y el soporte para la consola de gestión EPO, IPS, Filtrado Web y Email

Así mismo, el adjudicatario proporcionará a la APA el código de contrato de mantenimiento, código de cliente o identificación equivalente que permita acceder directamente desde la página web del fabricante a los servicios asociados al mantenimiento de las licencias.

3.1 Informes

El contratista está obligado a entregar los informes que a continuación se describen de manera bimensual el primer día hábil o en un plazo de 24 horas si existiera un problema severo que impida a la APA ejecutar tareas, de cualquier tipo, que requieran el uso del equipamiento objeto de soporte (incidencias críticas), desde que se solicite formalmente por parte de la APA.

Para los informes que deban ser entregados de manera inmediata (los que se definen a continuación como "Informes de Incidencias" se considera ésta dentro del plazo de 24 horas desde su solicitud formal por parte de la APA.

Los informes que se deberán entregar en soporte magnético compatible con las aplicaciones software instaladas en la citada Administración son los siguientes:

- **Informes de incidencias.** Se entregarán informes de las incidencias graves (críticas, altas y medias) que afecten al servicio que permitan determinar el impacto y causas de las mismas. Un informe concreto dentro de este epígrafe será el "informe de fallos y trabajos sobre gestión de resolución de incidencias" que deberá entregarse 24 horas tras la detección de la incidencia, salvo casos de alto impacto en los que se requerirá una respuesta inferior a 8 horas.

- **Informes de riesgos, vulnerabilidades y fallos de seguridad.** Se entregarán informes y enviarán alertas de los riesgos, vulnerabilidades y fallos de seguridad detectados, incluidos exploits de día cero, que afecten, directa o potencialmente, a los equipos objeto del contrato. Estos informes y alertas deberán entregarse de forma inmediata una vez detectado el riesgo, vulnerabilidad o fallo de seguridad.

4. *NIVELES DE SERVICIO*

1.1. Aspectos generales

Los servicios estarán sometidos a un acuerdo de nivel de servicio en base al cual se regirá el seguimiento del servicio, su proceso de mejora continua y la aplicación de las cláusulas de penalización.

La empresa adjudicataria se compromete a cumplir el Acuerdo de Nivel de Servicio en los términos establecidos en el presente pliego.

El responsable del contrato, o en su defecto la persona (o personas) en la que pueda delegar esta actividad, supervisarán el cumplimiento del Acuerdo de Nivel de Servicio (ANS).

El incumplimiento del ANS dará lugar a la imposición de las penalidades establecidas o a la resolución del contrato.

En cualquier caso siempre serán potestad de la APA las determinaciones finales sobre el cumplimiento del acuerdo de nivel de servicio.

El incumplimiento del nivel de servicio exigido, indicado en este apartado, dará lugar a la imposición de las penalidades que se indican en el pliego de cláusulas administrativas.

1.2. Acuerdo de nivel de servicio

1.2.1. Disponibilidad de nuevas versiones

El plazo de disponibilidad de una nueva versión de software o actualización de alguna funcionalidad asociada amparada por este contrato se define como el tiempo transcurrido desde que el fabricante publica en su página web o repositorio oficial de información el anuncio de disponibilidad de la nueva versión hasta que la descarga de la misma es accesible para la APA

En todos los casos este plazo de disponibilidad de nuevas versiones debe ser inferior a 24 horas, salvo en situaciones críticas identificadas por la APA como tales, en cuyo caso, dicha disponibilidad deberá ser inferior a 5 horas.

Oviedo, 29 de junio de 2018

Luis Alberto Fernández Ardura
RESPONSABLE DE PROYECTOS

VºBº

Javier Rojo Fernández
JEFE DEL SERVICIO DE SEGURIDAD