UNIÓN EUROPEA

ctnet

Red de Ciencia, Tecnología y Sociedad de la Información Región de Murcia

CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL

Pliego de Cláusulas Administrativas y Prescripciones Técnicas

Región de Murcia

fundación Integra _digital

Ref: PA-20-AFP
Fecha: octubre 2020

INDICE

Introducción.

El objetivo 1 de la Agenda Digital para España se orienta a "Fomentar el despliegue de redes y servicios para garantizar la conectividad digital". El objetivo 5, por su parte, a "Impulsar el sistema de I+D+i en Tecnologías de la Información y las Comunicaciones", una de cuyas líneas de actuación hace referencia a la necesidad de "fomentar la colaboración entre las PYME y los centros de investigación". Adicionalmente, el Plan de telecomunicaciones y redes ultrarrápidas recoge en su "Eje III. Impulso a la demanda" medidas para, en estrecha colaboración con las CC.AA., dotar de conectividad de banda ancha ultrarrápida a los centros escolares y otros centros públicos relevantes y facilitar la instalación de infraestructuras tecnológicas que permitan el uso intensivo y concurrente de aplicaciones y contenidos digitales en dichos centros.

Con fecha 7 de marzo de 2014, el Consejo de Gobierno de la Región de Murcia aprobó la Estrategia de Investigación e Innovación para la Especialización Inteligente de la Región de Murcia (RIS3Mur) que define los sectores estratégicos en el contexto económico regional en el ámbito de la investigación e innovación, que concentrarán mayoritariamente las acciones a desarrollar con los fondos europeos, designando específicamente la red CTnet como infraestructura regional de telecomunicaciones de la investigación.

Con fecha 18 de marzo de 2014, se presentó el Plan Estratégico de la Región de Murcia 2014-2020, el cual se estructura en 7 líneas estratégicas. La línea estratégica número 5 del citado Plan, Infraestructuras, contempla en su apartado 5.6 "Mejorar las Infraestructuras Productivas", incluyendo en sus recomendaciones "Priorizar el despliegue de redes de telecomunicaciones de banda ancha en los parques industriales".

Con fecha 13 de mayo de 2015 la Comisión Europea aprobó el Programa Operativo en el marco del objetivo de inversión en crecimiento y empleo para Murcia en el periodo 2014-2020. Dentro del Objetivo Temático 2 "Mejorar el uso y calidad de las tecnologías de la información y de la comunicación y el acceso a las mismas", se incluye como prioridad de inversión 2a "La ampliación de la implantación de la banda ancha y la difusión de redes de alta velocidad y el respaldo a la adopción de tecnologías emergentes y redes para la economía digital". Esta actuación se encuadra dentro del objetivo específico OE.2.1.1 "Fomentar el despliegue y adopción de redes y servicios para garantizar la conectividad digital."

La red de Ciencia, Tecnología y Sociedad de la Información de la Región de Murcia (Red CTnet Ultrarrápida), gestionada por la Fundación Integra, presta servicio, entre otros, a la totalidad de centros educativos de primaria y secundaria integrados en el proyecto Escuelas Conectadas para su conexión a la Red de I+D+i nacional (RedIRIS Nova). La Fundación Integra dispone de cuatro equipos Palo Alto de la serie PA y una consola Panorama del mismo fabricante para la gestión centralizada. El objeto de este procedimiento abierto es la adquisición de equipamiento informático asociado a la seguridad de las comunicaciones de la Red CTnet Ultrarrápida, en concreto, la ampliación de la capacidad del firewall perimetral de la Fundación Integra mediante la adquisición de un nuevo equipo para proteger el tráfico intercambiado por el proyecto Escuelas Conectadas con el exterior (RedIRIS e Internet comercial). Este pliego

describe el alcance, objetivos generales, suministros a realizar, presupuesto y plazo de ejecución de la presente contratación. Asimismo, se especifican las condiciones que deben cumplir los licitadores y los aspectos por los que se regirán las relaciones entre la Fundación Integra y el adjudicatario, durante la prestación de los servicios.

El proyecto está financiado con fondos europeos FEDER de la Unión Europea en un 80 %, y en un 20 % por fondos propios de la Consejería de Presidencia y Hacienda, a través de la Dirección General de Estrategia y Transformación Digital, estando coordinado por la Fundación Integra.

Cláusula 1ª.- Objeto.

La Fundación Integra, que es una entidad sin ánimo de lucro perteneciente al Sector Público Regional, en régimen de derecho privado, constituida para contribuir a la modernización de la Región de Murcia, en base a la integración de recursos y Nuevas Tecnologías de la información y de las comunicaciones, convoca procedimiento abierto con el siguiente objeto:

Contratación de la ampliación del firewall perimetral

Este suministro se considera que se corresponde con el código CPV 32420000-3 (suministro equipo de red).

Esta contratación se efectuará con estricta sujeción al presente Pliego de Cláusulas Administrativas y Prescripciones Técnicas.

Cláusula 2ª.- Vigencia del contrato y Plazos de Ejecución.

a) Vigencia. La vigencia del contrato se fija desde la fecha de firma del contrato hasta la finalización del período de garantía contratado.

b) Plazos de Ejecución. El suministro e instalación de equipamiento deberá realizarse en un período de 6 semanas a partir de la fecha de firma del contrato y siempre antes del 31 de diciembre de 2020.

Cláusula 3ª.- Precio de Licitación.

El precio máximo de licitación queda fijado en **Cincuenta y un mil euros (51.000,00 €)**. En esta cantidad **no está incluido** el correspondiente Impuesto de Valor Añadido (I.V.A.).

Cláusula 4ª.- Financiación del contrato.

La financiación de este contrato corre a cargo de la Fundación Integra y está

supeditada a la transferencia a dicha Fundación de la aportación de capital de la partida 13.04.00.521A.731.06 con número de proyecto 43700 de los presupuestos generales de la Comunidad Autónoma de la Región de Murcia para el ejercicio 2020, para el desarrollo de la actuación "A la Fundación Integra. Red de Ciencia, Tecnología y Sociedad de la Información, CTnet ultrarrápida".

Dicha actuación está financiada con fondos europeos FEDER de la Unión Europea en un 80 %, y en un 20 % por fondos propios de la Consejería de Presidencia y Hacienda, a través de la Dirección General de Estrategia y Transformación Digital.

Cláusula 5ª.- Forma de pago del precio.

El pago del importe del suministro objeto de la presente contratación se efectuará a la finalización del mismo, mediante transferencia, una vez que la CARM haya transferido a la Fundación Integra los fondos necesarios para atender la factura emitida por el Adjudicatario. Para proceder al pago, la factura deberá estar aprobada por el Director Gerente de Fundación Integra previo informe favorable del Responsable del Proyecto.

Cláusula 6ª.- Obligaciones del adjudicatario.

El adjudicatario se obliga al cumplimiento, bajo su exclusiva responsabilidad, de las disposiciones vigentes o que dicten en el futuro sobre relaciones laborales, generales o derivadas de convenios colectivos; sobre seguridad social; de seguridad y de salud en el trabajo; de carácter fiscal y de cualquier otra que sea necesaria para la realización de los trabajos.

El adjudicatario se obliga asimismo al cumplimiento, bajo su exclusiva responsabilidad, de las disposiciones vigentes en cada momento sobre Protección de Datos de Carácter Personal, con relación a todos los datos que tuviere que manejar con motivo de este contrato. Se exigirá el cumplimiento de los requerimientos de la Ley Orgánica de Protección de Datos (LOPD) y de la Ley de Servicios de la Sociedad de la Información (LSSI).

Durante la vigencia del contrato, el adjudicatario queda obligado a presentar, previo requerimiento de la Fundación Integra, las declaraciones o documentos que acrediten el cumplimiento de sus obligaciones fiscales, tales como Impuesto sobre la Renta de las Personas Físicas, Impuesto sobre Sociedades, Impuesto sobre el Valor Añadido; así como las de Seguridad Social y aquellas otras que la Fundación Integra estime oportunas.

La Fundación Integra queda exenta de cualquier responsabilidad que pudiera derivarse como consecuencia del incumplimiento por parte del adjudicatario de las obligaciones indicadas anteriormente y de cualquier otra que le pudiera corresponder.

Cláusula 7ª.- Lotes.

La presente contratación se adjudicará de forma global, sin lotes, al tratarse de un

único equipo.

Cláusula 8ª.- Concurrencia y solvencia.

Concurrencia.

Podrán licitar todas las personas jurídicas **en cuyo objeto social figuren las actividades correspondientes para el correcto desempeño de los servicios objeto de la presente licitación**, y que dispongan de recursos suficientes (personal, equipamiento, etc.) para su adecuada ejecución.

Dichas personas jurídicas se podrán presentar de forma individual o mediante alguna asociación o agrupación que tenga carácter jurídico a efectos de contratación.

Cualquier licitador sólo podrá presentar una propuesta, tanto si lo hace de forma individual como si lo hace dentro de alguna asociación o agrupación que tenga carácter jurídico a efectos de contratación. **La contravención a esta norma será motivo de exclusión del procedimiento abierto de todas las ofertas en que participe.**

Solvencia técnica

Dada la importancia de la red CTnet y de las instituciones a las que interconecta, el número de usuarios a los que presta servicio, su carácter de Sector Público Regional y el elevado nivel de disponibilidad que se le exige, los licitadores deberán acreditar adecuadamente su solvencia técnica debiendo, para ello, presentar en la **documentación administrativa (sobre nº 1)** documentación acreditativa del nivel de cualificación/especialización que ostenta como partner del fabricante del equipamiento ofertado. Solo se admitirán ofertas de partners del nivel máximo de cualificación/especialización del correspondiente fabricante.

Solvencia económica

Se acreditará mediante: volumen anual de negocios de la empresa en el ámbito al que se refiere este contrato (suministro e instalación de equipos de red) referido al mejor ejercicio de los 3 últimos disponibles, por importe igual o superior a 76.500,00€, IVA excluido. El volumen anual de negocios mínimo exigido se acreditará mediante relación de los principales suministros efectuados.

Cláusula 9ª.- Prescripciones Técnicas.

9.1 Objeto de contratación

La Fundación Integra dispone de cuatro equipos Palo Alto de la serie PA y de una consola Panorama del mismo fabricante para la gestión centralizada. **Es objeto de contratación del presente procedimiento la ampliación de capacidad de dicho firewall perimetral mediante la adquisición de un nuevo equipo que se instalará en paralelo con los anteriores, con el fin de aumentar el throughput total de la**

plataforma. **Este nuevo equipo deberá ser integrado en la gestión de la consola Panorama del fabricante Palo Alto de la que se dispone, con el fin de poder realizar de forma centralizada la gestión integral de las políticas de los equipos que conforman el firewall perimetral, el licenciamiento de todos los equipos y generar informes y estadísticas conjuntas agregando la información de todos ellos.**

El suministro **incluirá los trabajos de instalación (para lo que deberán de aportar todos los elementos físicos necesarios, tales como raíles para rack de 19", tornillos, tuercas, etc.), configuración, pruebas y puesta en marcha**. **Es también objeto de contratación la garantía del equipo adquirido en las condiciones que se especifican más adelante. Todos los elementos integrantes de la oferta han de ser nuevos y originales del fabricante**.

Por último, es objeto de contratación una **formación** en materia de configuración y administración del equipamiento y su software asociado, con una duración de 4 horas online.

El firewall ofertado deberá cumplir los siguientes **requisitos mínimos necesarios**:

a) HARDWARE

- Instalación en rack de 19" (máximo 3Us por insuficiencia de espacio en rack).
- 4 puertos 100/1000 RJ45.
- 16 puertos 1/10 Gigabit SFP/SFP+, con cuatro puertos habilitados con transceptores 10G-SR.
- 4 puertos 40G QSFP+.
- Sistema operativo almacenado en dispositivos de alta velocidad redundados por RAID 1 o similar.
- Puerto dedicado para gestión "fuera de banda".
- Puerto de consola.
- Arquitectura hardware separada para gestión y servicio, tanto a nivel de interfaces de red como de CPU, memoria y discos dedicados independientes, que en ningún caso se compartan con el plano de datos, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa y que pueda reiniciarse el plano de datos sin afectar al plano de gestión.
- Fuentes de Alimentación Redundadas Hot-swap
- Ventiladores redundados Hot-Swap

b) CARACTERÍSTICAS DE NETWORKING

- Integración en modo L2, L3, Tap y modo transparente (L1), tanto en IPv4 como IPv6. Para el caso de la integración en modo transparente (L1) es

necesario que se replique el estado (up/down) de una interfaz a otra.

- Capacidad de Virtual Routers para la creación de tablas de routing separadas y aisladas que puedan alimentarse mediante routing estático y/o dinámico (RIP, OSPFv2/v3 y BGP con reinicio "graceful").
- Policy-based forwarding en base a uno o varios de los siguientes criterios:
    - la IP de origen o red
    - la aplicación, categoría o grupo de aplicación
    - el usuario o grupo de usuarios.
- Bidirectional Forwarding Detection (BFD).
- Soporte de IPv6 en cualquiera de los modos de integración.
- IPSEC VPN.
- SSL VPNs.
- Soporte de VLAN's (802.1q) con el rango 0-4.094.
- Agregación de enlaces mediante el protocolo LACP (802.3ad).
- NAT y PAT.
- Posibilidad de mecanismos de alta disponibilidad tanto en modo activo/activo como activo/pasivo (para el caso de que la Fundación Integra adquiera un segundo equipo de idénticas características en el futuro).

c) GESTIÓN Y ADMINISTRACIÓN

- Gestión y administración por medio de interface web y a través de línea de comandos.
- Capacidad para ser gestionado de forma integral junto con el resto de equipos del firewall perimetral de CTnet mediante un equipo Panorama del fabricante Palo Alto.
- Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.
- Capacidad de realizar, visualizar y validar cambios de configuración antes de aplicarlos (commit). Se debe también tener la capacidad de almacenar configuraciones anteriores, pudiendo aplicarlas en caso de ser necesario (rollback).
- API XML abierta y documentada (RESTFul) para la integración con aplicaciones externas. La API debe permitir operaciones de lectura (recibir datos estadísticos), operaciones de escritura (modificar la configuración), cambios de objetos y la generación de informes (reports).
- Capacidad de envío de logs vía SYSLOG para retención y posterior tratamiento, pudiendo seleccionar el tipo de log, y poder definir filtros que seleccionen los eventos que deben exportarse.
- Soporte SNMP incluyendo la capacidad de obtener estadísticas relativas a

los procesos de recolección de logs y del estado de salud de las funciones de alta disponibilidad.

- Capacidad de agrupar interfaces del propio firewall en conjuntos independientes formando zonas, de forma que las políticas de seguridad se definan por zonas pudiendo incluir en las mismas políticas varias zonas origen y destino para el análisis de tráfico y procesado de reglas de seguridad, así como la posibilidad de crear múltiples reglas de seguridad entre zonas origen y destino o incluir cualquier zona origen o destino de tráfico en dichas reglas.
- Capacidad para definir la política de seguridad mediante reglas y perfiles de seguridad en una única tabla centralizada donde se establezca toda la configuración.

d) CARACTERÍSTICAS DE SEGURIDAD

Si las funcionalidades que se indican a continuación necesitan ser licenciadas, la licencia correspondiente ofertada no podrá limitar ni el número de IPs ni el número de usuarios protegidos.

En la descripción de estos requisitos mínimos donde dice “Capacidad” se entenderá que dicha funcionalidad debe venir incluida en la solución ofertada, mientras que si se habla de “Posibilidad” debe entenderse que la solución ofertada no tiene por qué soportar dicha funcionalidad de base pero sí con licenciamiento adicional futuro.

Identificación y control de aplicaciones

- Capacidad de identificación de aplicaciones a nivel 7, así como la identificación de subfunciones dentro de una aplicación como por ejemplo “compartir escritorio de webex”, “chat dentro de webex”, “transferencia de ficheros en webex”, etc.
- Capacidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.
- Capacidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.
- Capacidad de identificar aplicaciones propietarias que usen los protocolos HTTP y TCP.

Protección ante vulnerabilidades

- Capacidad de aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten

en el tráfico bien entrante o saliente de/hacia Internet sin incurrir en latencia para no penalizar la experiencia de navegación del usuario. En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas. Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades especificando si son vulnerabilidades que aplican a los clientes, los servidores o a ambos indistintamente.

- Capacidad de categorizar las vulnerabilidades por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.
- Capacidad de usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.

Filtrado de URL's

- Posibilidad de crear políticas basadas en control por URL'S y/o categorías de URL's para aplicarlas a la navegación http o https, permitiendo o bloqueando el acceso de los usuarios a determinadas páginas.
- En caso de bloqueo, debe poder personalizarse la página mostrada al usuario, así como debe existir la posibilidad de solicitar la reclasificación de falsos positivos y negativos.
- Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

Antivirus

- Capacidad de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

- Capacidad para aplicar las políticas de antivirus de forma granular, permitiendo, por ejemplo, la aplicación de dichas políticas a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

Tecnología de SandBoxing

- Posibilidad de disponer de un servicio en la nube para analizar ficheros de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

Se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

- Posibilidad de que el análisis realizado por este servicio en la nube, en caso de que la información enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad, deberá generar las firmas apropiadas en un plazo inferior a 10 minutos, que se utilizarán para actualizar los motores propios de antivirus, amenazas y filtrado URL, de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas.

Bloqueo de ficheros y datos sensibles

- Capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo. Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de ficheros y se generen los logs correspondientes.

- También se requiere la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito de forma que se evite la filtración al exterior de este tipo de datos.

Inspección SSL

- Capacidad de inspeccionar el tráfico SSL para analizar las comunicaciones y aplicar las funcionalidades de seguridad anteriores.

Detección de equipos comprometidos en la red

- Capacidad de uso de motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con indicación de tiempos, usuarios, direcciones IP y vulnerabilidades o amenazas detectadas.

Seguridad DNS

- Capacidad de habilitar mecanismos de DNS sinkholing que permitan interceptar las peticiones de resolución de nombre asociados a amenazas (botnets, malware, virus, etc..). Las firmas DNS deben permitir detectar

técnicas de ocultación utilizadas por las amenazas como DGA/DNS tunneling aprovechando técnicas de análisis avanzado mediante machine learning con la información compartida por múltiples usuarios. Las firmas DNS se deberán crear y actualizar de forma automática.

- Para garantizar el adecuado nivel de protección de esta funcionalidad, al crecer exponencialmente el número de firmas DNS necesarias y no poder almacenarse localmente, deberá existir la posibilidad de realizar consultas en tiempo real de dominios contra un servicio en la nube del fabricante.

Protección ante ataques de DDoS

- Capacidad de protección ante ataques de Denegación de Servicios de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las direcciones IP origen y destino a inspeccionar o el usuario interno de la red que puede estar originando el ataque. Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

Informes

- Capacidad de generar informes tanto predefinidos como personalizados utilizando los logs. Los informes podrán generarse tanto manualmente como de forma automática y programada. También podrá agruparse varios informes en un único documento con formato PDF.

e) OTRAS CARACTERÍSTICAS

Virtual Systems

- Capacidad para la definición de instancias de firewall virtual en un mismo hardware físico. Cada instancia debe ser independiente, y gestionada de forma separada y el tráfico aislado del resto. Como mínimo se requieren 10 instancias.

Captura de tráfico

- Capacidad de realizar capturas del tráfico que atraviesa sus interfaces en formato PCAP, de forma que se puedan establecer filtros de captura basados en IP y puerto origen/destino, aplicación, etc.

Geo-Localización

- Capacidad para la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- Capacidad de visualización de los países de origen y destino en la vista detallada de los logs de cualquier funcionalidad de seguridad.

Integración con listas dinámicas de IPs de terceros

- Capacidad para descargar listas dinámicas de IPs de terceros por comando o vía web (sin necesidad de hacer uso del API XML, tan solo indicando la URL de descarga), que se actualicen de manera automática, para incorporar inteligencia sobre orígenes o destinos maliciosos provenientes de otros servicios.

f) FUNCIONALIDAD, CAPACIDAD Y RENDIMIENTO

El equipo deberá estar licenciado con la funcionalidad de Threat Prevention o similar (inspección de todo el tráfico independientemente del puerto o protocolo utilizado o de si está o no encriptado y bloqueo automático de vulnerabilidades conocidas, malware, spyware, etc) por 1 año. No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, control de archivos, …). Se entiende por tanto que los rendimientos solicitados utilizan todas las firmas disponibles para cada mecanismo.

Descripción	Características mínimas requeridas
Threat prevention (o licencia similar) throughput	10 Gbps
IPSec VPN throughput	11Gbps
Nº máximo de sesiones soportadas	4.000.000
Nuevas conexiones por segundo	180.000

9.2. Garantía

Todo el equipamiento ofertado deberá contar con un soporte y garantía del fabricante **24x7** en caso de avería o malfuncionamiento durante 1 año con tiempo de reemplazo NBD. El adjudicatario deberá hace entrega a la Fundación Integra de la documentación acreditativa de la garantía de los equipos adquiridos, en la que deberá reflejarse claramente el compromiso asumido respecto al nivel de servicio.

Cláusula 10ª.- Ubicación del suministro.

El suministro de equipamiento se realizará en el CPD de CTnet, ubicado en el Parque Científico de Murcia, Complejo Espinardo. Edificio S. Carretera de Madrid Km 388.

Cláusula 11ª.- Proposiciones.

a) Las proposiciones para tomar parte en este procedimiento abierto se presentarán en sobre cerrado en los locales de la Fundación Integra (C/Manresa 5, Entlo dcha, 30004 MURCIA) antes de las **11:00h del día 12 de noviembre de 2020**. A las 11:00h se constituirá la Mesa de Contratación y se harán públicos los nombres de las empresas que han presentado oferta.

b) Cada licitador únicamente podrá presentar una proposición económica, sin variantes, según modelo indicado posteriormente, y una proposición técnica, sin variantes. No podrá suscribirse a ninguna propuesta de unión temporal con otros, si ya lo ha hecho individualmente o ya figura en otra unión temporal.

c) **En el referido sobre figurará la leyenda**: "Proposición que presenta D. ….. (en representación de … en caso de persona jurídica o agrupación) para tomar parte en el procedimiento abierto convocado por la Fundación Integra para la *"CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL"*.

   Dentro de este sobre mayor se contendrán tres sobres cerrados en los que figurará la misma inscripción referida en el apartado anterior y un subtítulo, tal y como se detalla en las tres cláusulas siguientes. Toda la documentación que se presente por los licitadores deberá estar redactada en castellano.

Cláusula 12ª.- Contenido del Sobre nº1. DECLARACIÓN RESPONSABLE / DOCUMENTACIÓN ACREDITATIVA

En el referido sobre cerrado figurará la leyenda:

"Proposición que presenta D. ….. (en representación de …, en su caso, de persona jurídica o agrupación) para tomar parte en el procedimiento abierto convocado por la Fundación Integra para la "CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL".

Este sobre se identificará como "DECLARACIÓN RESPONSABLE / DOCUMENTACIÓN ACREDITATIVA"

En el referido sobre cerrado se incluirá:

- Copia del DNI de la persona que presenta la oferta
- Certificación registral de poder o escritura de poder, indicando con un SEPARADOR, las páginas de dicha escritura donde figure el NOMBRE Y

PODERES DEL PROPONENTE.

- Escritura de constitución de la Sociedad, y en su caso, aquella otra más reciente en la que figuren actualizados sus estatutos, inscrita en el registro que corresponda, bien en el mercantil o en de las sociedades cooperativas, cuando concurra una sociedad de esta naturaleza, indicando con un SEPARADOR, las páginas de dicha escritura en la que figure el OBJETO SOCIAL DE LA SOCIEDAD.
- Declaración responsable firmada.
- La documentación de solvencia técnica y económica a la que hace referencia la Cláusula 8ª.

Para la presentación de esta documentación se seguirá lo dispuesto en el artículo 140 de la Ley 9/2017 de Contratos del Sector Público, esto es:

El licitador deberá firmar la declaración responsable, **según el formulario de documento europeo único,** referido a este procedimiento de contratación, y cuyo modelo al que debe ajustarse está disponible en fichero electrónico anexo a éste y en la que el licitador ponga de manifiesto lo siguiente:

- Que la sociedad está válidamente constituida y que conforme a su objeto social puede presentarse a la licitación, así como que el firmante de la declaración ostenta la debida representación para la presentación de la proposición y de aquella.

- Que cumple los requisitos de solvencia económica, financiera y técnica o profesional exigidos, en las condiciones que establezca el pliego de conformidad con el formulario normalizado del documento europeo único de contratación.

- Que no está incursa en prohibición de contratar por sí misma ni por extensión como consecuencia de la aplicación del artículo 71.3 de la Ley 9/2017.

- La designación de una dirección de correo electrónico en que efectuar las notificaciones

En los casos en que el empresario recurra a la solvencia y medios de otras empresas de conformidad con el artículo 75 de la Ley 9/2017, cada una de ellas también deberá presentar una declaración responsable en la que figure la información pertinente para estos casos con arreglo al formulario normalizado del documento europeo único de contratación. La presentación del compromiso a que se refiere el apartado 2 del artículo 75 se realizará de conformidad con lo dispuesto en el apartado tercero del artículo 140 de la Ley 9/2017.

En todos los supuestos en que varios empresarios concurran agrupados en una unión temporal, se aportará una declaración responsable por cada empresa participante en la que figurará la información requerida en estos casos en el formulario del documento europeo único de contratación. Adicionalmente a la declaración o declaraciones a que se refiere el párrafo anterior se aportará el compromiso de constituir la unión temporal por parte de los empresarios que sean parte de la misma de conformidad con lo exigido en el apartado 3 del artículo 69 de la Ley 9/2017. Para este documento se puede utilizar el modelo propuesto en la web de la Fundación Integra,

www.f-integra.org, en la sección perfil de contrataciones.

Cláusula 13ª.- Contenido del Sobre nº2. PROPUESTA TÉCNICA

En el referido sobre cerrado figurará la leyenda:

"Proposición que presenta D. ….. (en representación de …, en su caso, de persona jurídica o agrupación) para tomar parte en el procedimiento abierto convocado por la Fundación Integra para la "CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL".
Este sobre se identificará como "PROPUESTA TÉCNICA"

Contendrá **original impreso en papel** de la propuesta técnica, que será tal que satisfaga como mínimo la totalidad de los requisitos básicos y que deberá ajustarse al modelo indicado en el Anexo I.

Cláusula 14ª.- Contenido del Sobre nº3. PROPUESTA ECONÓMICA

En el referido sobre cerrado figurará la leyenda:

"Proposición que presenta D. ….. (en representación de …, en su caso, de persona jurídica o agrupación) para tomar parte en el procedimiento abierto convocado por la Fundación Integra para la "CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL".
Este sobre se identificará como "PROPUESTA ECONÓMICA".

Dicho sobre contendrá la propuesta económica del licitador, que se formulará conforme al modelo que figura a continuación:

PROPUESTA ECONÓMICA

Don .....……., mayor de edad, vecino de ....., provincia de ……., con domicilio en C/....., número ….., con D.N.I. nº....., en plena posesión de mis capacidades jurídicas y de obrar, en nombre propio (o en el caso de actuar en representación: como apoderado de ....., con domicilio en …….., calle ……, número …., C.I.F. o D.N.I. nº……..), conforme acredito con poder notarial declarado bastante, enterado del anuncio publicado en ....., y de las condiciones y cláusulas para concurrir al Procedimiento abierto para la *"CONTRATACIÓN DE LA AMPLIACIÓN DEL FIREWALL PERIMETRAL"* acudo como licitador al mismo.

A este efecto hago constar que conozco el Pliego de Cláusulas Administrativas y Prescripciones Técnicas que sirven de base a la convocatoria, que acepto

incondicionalmente todas sus cláusulas, comprometiéndome en nombre propio (o "de la Empresa xxxxxx que represento") a tomar a mi cargo el mencionado proyecto, con estricta sujeción a las expresadas condiciones y cláusulas, por el siguiente precio:

IMPORTE (en letra)…..……....EUROS, (XXX.XXX,XX €)

En esta cantidad no se incluye el Impuesto sobre el Valor Añadido (IVA), 21%

IMPORTE TOTAL (IVA incluido) (en letra)……..EUROS**,** (XXX.XXX,XX €)

Lugar, fecha y firma del proponente

Cláusula 15ª.- Mesa de Contratación.

Estará formada por un Presidente y dos Vocales, miembros que serán designados por:

- Un miembro por parte de la Dirección General de Estrategia y Transformación Digital de la Consejería de Presidencia y Hacienda.
- Dos miembros por parte de la Fundación Integra.

Cláusula 16ª.- Apertura de proposiciones.

Una vez constituida, la Mesa de Contratación procederá a la revisión y calificación de la documentación del sobre nº1 comunicando por correo electrónico a los licitadores los defectos u omisiones subsanables, concediéndose, en su caso, un plazo máximo de 3 días hábiles para subsanación.

La admisión definitiva al procedimiento abierto de las ofertas con defectos subsanables estará condicionada a la subsanación en plazo y forma de dichos. En caso contrario quedarán excluidas del procedimiento abierto.

Finalizada la fase de subsanación de ofertas, en acto público que tendrá lugar en la fecha y hora que se comunique oportunamente, se procederá a la apertura de los sobres de las proposiciones económicas y técnicas. A continuación, se dará por terminado el acto público para proceder a la valoración de las mismas.

Cláusula 17ª.- Criterios de Valoración.

La selección de la empresa adjudicataria del presente procedimiento abierto, se realizará de acuerdo con las puntuaciones obtenidas en la valoración de las ofertas presentadas, siendo el adjudicatario el licitador cuya oferta obtenga la mayor puntuación.

El resultado final (máximo 100 puntos) se obtendrá como suma de las valoraciones de los siguientes apartados:

Criterios sometidos a juicio de valor: no hay.

Criterios de valoración directa:

Proposición Técnica:	**Máximo:**	**10 puntos**
Proposición Económica:	**Máximo:**	**90 puntos**

Las **Proposiciones Técnicas** se valorarán de la siguiente manera: por cada 2 puertos 10 Gigabit adicionales habilitados con transceptores 10G-SR se otorgarán 5 puntos, hasta un máximo de 10 puntos, que se corresponderán con 4 puertos 10 Gigabit adicionales habilitados con transceptores 10G-SR.

Las **Proposiciones Económicas** se valorarán de forma lineal al descuento ofertado sobre el presupuesto de licitación, asignándose el máximo de puntos a la oferta de mayor descuento y 0 puntos a ofertas iguales al importe del presupuesto, esto es, sin descuento. Los cálculos se harán considerando los porcentajes de descuento de las ofertas presentadas. No se tomará en consideración ninguna oferta que supere el precio de licitación.

Ofertas anormalmente bajas: Se considerarán, en principio, anormalmente bajas las ofertas cuyo descuento (porcentual) en el precio ofertado sea superior en más de 10 unidades (porcentuales) al de la mediana de las ofertas presentadas.

En caso de oferta anormalmente baja, conforme a los criterios señalados, se dará audiencia al licitador para que pueda justificar la valoración económica (Precio), precisando las condiciones de la misma y demás aspectos que señale la Fundación Integra. Si la Fundación Integra considera que la oferta anormal no puede ser cumplida, acordará la adjudicación a la oferta siguiente, de acuerdo con el orden de clasificación.

En caso de coincidencia numérica en la puntuación final se seguirán los criterios de desempate previstos por la Ley de Contratos 9/2017 en el artículo 147.2.

17.3. Solicitud de información adicional

Fundación Integra se reserva el derecho a solicitar al licitador cuya proposición haya obtenido la mayor puntuación la información que precise y que estime pertinente para comprobar la veracidad y cumplimiento de aquellos requisitos establecidos en la Cláusula de Prescripciones Técnicas o solicitados para su valoración (en adelante, "la Información").

En el caso de que Fundación Integra solicite dicha Información, el licitador deberá presentarla en el plazo que se señale en la solicitud. El licitador deberá presentar la Información únicamente dando respuesta a los requerimientos planteados por Fundación Integra sin que sea posible incorporar información o documentación adicional no solicitada por dicha entidad. Asimismo, Fundación Integra podrá solicitar la Información de forma estructurada y con formatos normalizados.

La Fundación Integra se reserva igualmente el derecho a validar técnicamente aquella proposición que haya obtenido la mayor puntuación. En tal caso, el equipo ofertado deberá someterse a unas pruebas de validación en las que se comprobará el cumplimiento de las funcionalidades mínimas exigidas por este pliego, descritas en el

Anexo II. Para ello, la Fundación Integra requerirá al licitador cuya proposición haya obtenido la mayor puntuación para que en un máximo de 5 días hábiles y sin coste para la Fundación Integra, desplace un técnico a las dependencias del Parque Científico de Murcia (CPD Edificio S. Complejo Espinardo. Carretera de Madrid Km 388. 30100 Espinardo (Murcia)) y configure una maqueta de pruebas con el equipamiento ofertado. Las pruebas de validación se llevarán a cabo bajo supervisión de los técnicos de la Fundación Integra. Superadas estas pruebas en su totalidad, los técnicos de la Fundación Integra emitirán el correspondiente informe favorable, que se entregará a la Mesa de Contratación. En caso contrario, o de que no se haya podido realizar la prueba de validación técnica por causas imputables al licitador, se notificará este extremo a la Mesa de Contratación, que procederá a excluir al licitador del presente procedimiento.

En el supuesto de que, tras las correspondientes comprobaciones, Fundación Integra comprobase que la proposición del licitador incumple alguno de los requisitos mínimos establecidos en el Pliego de Prescripciones Técnicas, dicha oferta no se tendrá en cuenta en el presente procedimiento de licitación. En este caso, la Fundación Integra podrá repetir este procedimiento con el siguiente licitador mejor puntuado (y así sucesivamente), al objeto de realizar las verificaciones que considere oportunas.

Cláusula 18ª.- Notificación de adjudicación y formalización del contrato.

Al propuesto como adjudicatario se le requerirá para que, dentro del plazo de diez días hábiles, **presente la documentación acreditativa** correspondiente al clausulado de este pliego. En el caso de defectos subsanables observados en los documentos presentados, se concederán 3 días hábiles para subsanación.

De no presentarse o no subsanar la documentación en el plazo señalado, se entenderá que el licitador propuesto como adjudicatario ha retirado su oferta y se requerirá la misma documentación al licitador siguiente por el orden en que hayan quedado clasificadas las ofertas.

Al propuesto adjudicatario, que no haya cumplimentado el requerimiento por causas imputables al mismo se le impondrá como penalidad el 3% del presupuesto máximo previsto, IVA excluido.

La resolución de adjudicación será motivada, atendiendo a la mayor puntuación total según los criterios indicados en este pliego y se notificará a los candidatos y licitadores.

La formalización se efectuará no más tarde de los 15 días hábiles siguientes a aquel en que se realice la notificación de la adjudicación a los licitadores.

Cláusula 19ª.- Causas sobrevenidas de rescisión del contrato por la Fundación Integra.

La Fundación Integra podrá suspender el contrato o resolverlo justificadamente por causas sobrevenidas y no imputables a la Fundación Integra, tales como:

- Modificación a la baja o congelación del presupuesto/partida de la CARM

asignado al proyecto para su anualidad de 2020.
- Supresión de la asignación presupuestaria por parte de la CARM al proyecto para su anualidad de 2020.
- Cualquier otra causa que derive en una situación equivalente a alguna de las 2 anteriores.

En caso de producirse alguno de estos supuestos, que serían comunicados al Adjudicatario con un mes de antelación, el Adjudicatario no tendrá derecho a reclamar por beneficios dejados de obtener, ni por otra causa, y solo recibirá como indemnización máxima por todos los conceptos el importe equivalente a los gastos en los que haya incurrido y justifique documentalmente.

Cláusula 20ª.- Propiedad Intelectual, uso y comercialización.

El adjudicatario acepta expresamente que la propiedad de todos los elementos, cualquiera que sea su naturaleza, elaborados al amparo del presente contrato corresponde a la Fundación Integra con exclusividad y a todos los efectos.

Asimismo, la Fundación Integra podrá explotar por cualquier medio audiovisual o escrito los desarrollos realizados al amparo de la presente contratación, sin menoscabo de los inalienables derechos de autor.

El adjudicatario garantiza a la Fundación Integra que dispone de los derechos de propiedad intelectual e industrial que sean precisos para la realización de cuanto es objeto del Contrato.

El adjudicatario será responsable de toda reclamación que pueda presentar un tercero por estos conceptos contra la Fundación Integra.

Cláusula 21ª.- Protección de Datos de Carácter Personal.

Todos los datos de carácter personal a los que tenga acceso la Fundación Integra (CIF G30583876) con motivo de esta contratación serán recogidos en ficheros de los que la propia Fundación es responsable con la exclusiva finalidad de servir de contacto con las personas implicadas y para registrar la firma del contrato en el caso de la oferta adjudicataria. Este tratamiento está legitimado por la propia ejecución del contrato en el que el firmante es parte y, por tanto, cuenta con el consentimiento del titular de los datos y podrá ser revocado en cualquier momento, sin perjuicio del mantenimiento de los datos por requisitos legales de otra índole que puedan existir.

La Fundación Integra no cederá datos de carácter personal a terceros sin consentimiento previo. Se podrán ejercitar los derechos de acceso, rectificación, limitación y supresión mediante carta postal con Fotocopia de DNI y datos de contacto a la dirección siguiente: C/ Manresa, 5 Entrlo. Drcha, CP 30004, Murcia o mediante escrito a la dirección datospersonales@f-integra.org. Así mismo se podrá ejercer el derecho de presentar una reclamación ante una autoridad de control.

Es responsabilidad de los ofertantes informar de todo lo anterior a las personas

físicas relacionadas con ellas cuyos datos vayan a ser suministrados a la Fundación en el transcurso del procedimiento negociado sin publicidad y los posibles trabajos o servicios derivados del mismo.

Cláusula 22ª.- Acciones de promoción y difusión.

Al tratarse de una actuación cofinanciada con Fondos FEDER, en las medidas de información y comunicación llevadas a cabo en este proyecto se debe cumplir con lo establecido en el apartado 2.2 del Anexo XII del Reglamento (CE) nº 1303/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013.

Para ello, el adjudicatario deberá seguir las indicaciones de la Fundación Integra en lo que se refiere a la publicidad y logotipos que deben aparecer en la documentación, cartelería, actividades y actos financiados que se realicen para el desarrollo de esta contratación.

En concreto, se incluirá logotipo de la Unión Europea (cumpliendo lo establecido en el Capítulo II del Reglamento de Ejecución UE Nº 821/2014 de la Comisión de 28 de julio de 2014), el lema "Fondo Europeo de Desarrollo Regional" y el lema "Una manera de hacer Europa".

Asimismo, se incluirán los logotipos de la CARM, Fundación Integra, así como relativos al proyecto o cualquier otro que se indique por parte de la Fundación Integra.

Todas las acciones, diseños gráficos y materiales utilizados para la difusión y promoción deberán contar con la aprobación y supervisión del Director de Proyecto designado por la Fundación Integra.

Cláusula 23ª Cumplimiento de obligaciones de carácter medioambiental, social y laboral

En virtud del artículo 201 de la Ley de Contratos del Sector Público de la Fundación Integra podrá tomar las oportunas medidas para comprobar, durante el procedimiento de licitación con respecto a los candidatos y durante la ejecución del contrato con respecto al contratista, que cumplen las obligaciones en materia medioambiental, social o laboral vigentes establecidas en el derecho de la Unión Europea, el derecho nacional, los convenios colectivos o por las disposiciones de derecho internacional medioambiental, social y laboral que vinculen al Estado.

El incumplimiento de las obligaciones referidas en el primer párrafo y, en especial, los incumplimientos o los retrasos reiterados en el pago de los salarios o la aplicación de condiciones salariales inferiores a las derivadas de los convenios colectivos que sea grave y dolosa, dará lugar a la imposición de las penalidades previstas en la citada Ley de Contratos del Sector Público.

Anexo I. Equipamiento ofertado. Modelo de Proposición Técnica

1. **Información sobre la empresa**.
   Datos que se estimen pertinentes para mostrar la capacidad y calidad de los trabajos desarrollados por la empresa licitadora (organización, proyectos relevantes, medios humanos, plan de aseguramiento de la calidad, trabajos realizados para la administración, etc.). En caso de que el licitador tenga previsto subcontratar algún servicio de los solicitados en este pliego, deberá indicar los datos relevantes de la empresa subcontratada.

2. **Características técnicas del equipo ofertado**.

Fabricante:	
Modelo:	

2.1 Hardware

Descripción	Características mínimas requeridas	OFERTADO
Instalación en rack de 19" (máximo 3Us por insuficiencia de espacio en rack).	Sí	(Sí/No)
Puertos 100/1000 RJ45.	4	
Puertos 1/10 Gigabit SFP/SFP+ totales / Nº puertos habilitados con transceptores 10G-SR.	16/4	
Puertos 40G QSFP+.	4	
Sistema operativo almacenado en dispositivos de alta velocidad redundados por RAID 1 o similar.	Sí	(Sí/No)
Puerto dedicado para gestión "fuera de banda".	Sí	(Sí/No)
Puerto de consola.	Sí	(Sí/No)
Arquitectura hardware separada para gestión y servicio, tanto a nivel de interfaces de red como de CPU, memoria y discos dedicados independientes, que en ningún caso se compartan con el plano de datos, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa y que pueda reiniciarse el plano de datos sin afectar al	Sí	(Sí/No)

plano de gestión.		
Fuentes de Alimentación Redundadas Hot-swap	Sí	(Sí/No)
Ventiladores redundados Hot-Swap	Sí	(Sí/No)

2.2 Funcionalidades, capacidad y rendimiento

a)CARACTERÍSTICAS DE NETWORKING

Características mínimas requeridas	**Características ofertadas**
Integración en modo L2, L3, Tap y modo transparente (L1). Para el caso de la integración en modo transparente (L1) es necesario que se replique el estado (up/down) de una interfaz a otra.	Cumple/no cumple URL donde se describa funcionalidad.
Capacidad de Virtual Routers para la creación de tablas de routing separadas y aisladas que puedan alimentarse mediante routing estático y/o dinámico (RIP, OSPFv2/v3 y BGP con reinicio “graceful”).	Cumple/no cumple. URL donde se describa funcionalidad.
Policy-based forwarding en base a uno o varios de los siguientes criterios: • la ip de origen o red • la aplicación, categoría o grupo de aplicación • el usuario o grupo de usuarios.	Cumple/no cumple (Indicar criterios soportados)
Bidirectional Forwarding Detection (BFD).	Cumple/no cumple
Soporte de IPv6 en cualquiera de los modos de integración.	Cumple/no cumple
IPSEC VPN.	Cumple/no cumple
SSL VPNs.	Cumple/no cumple
Soporte de VLAN’s (802.1q) con el rango 0-4.094.	Cumple/no cumple
Agregación de enlaces mediante el protocolo LACP (802.3ad).	Cumple/no cumple
NAT y PAT.	Cumple/no cumple
Posibilidad de mecanismos de alta disponibilidad tanto en modo activo/activo como activo/pasivo.	Cumple/no cumple

b) GESTIÓN Y ADMINISTRACIÓN

Características mínimas requeridas	Características ofertadas
Gestión y administración por medio de interface web y a través de línea de comandos.	Cumple/no cumple
Capacidad para ser gestionado de forma integral junto con el resto de equipos del firewall perimetral de CTnet mediante un equipo Panorama del fabricante Palo Alto con el fin de poder realizar de forma centralizada la gestión integral de las políticas de los equipos que conforman el firewall perimetral, el licenciamiento de todos los equipos y generar informes y estadísticas conjuntas agregando la información de todos ellos.	Cumple/no cumple URL donde se describa funcionalidad.
Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.	Cumple/no cumple URL donde se describa funcionalidad.
Posibilidad de realizar, visualizar y validar cambios de configuración antes de aplicarlos (commit). Se debe también tener la posibilidad de almacenar configuraciones anteriores, pudiendo aplicarlas en caso de ser necesario (rollback).	Cumple/no cumple URL donde se describa funcionalidad.
API XML abierta y documentada (RESTFul) para la integración con aplicaciones externas. La API debe permitir operaciones de lectura (recibir datos estadísticos), operaciones de escritura (modificar la configuración), cambios de objetos y la generación de informes (reports).	Cumple/no cumple URL donde se describa funcionalidad.
Posibilidad de envío de logs vía SYSLOG para retención y posterior tratamiento, con posibilidad de seleccionar el tipo de log, y poder definir filtros que seleccionen los eventos que deben exportarse.	Cumple/no cumple URL donde se describa funcionalidad.
Soporte SNMP incluyendo la posibilidad de obtener estadísticas relativas a los procesos de recolección de logs y del estado de salud de las funciones de alta disponibilidad.	Cumple/no cumple

c) CARACTERÍSTICAS DE SEGURIDAD

Identificación y control de aplicaciones

Características mínimas requeridas	Características ofertadas
Capacidad de identificación de aplicaciones a nivel 7, así como la identificación de subfunciones dentro de una aplicación.	Cumple/no cumple URL donde se describa funcionalidad.
Capacidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.	Cumple/no cumple. URL donde se describa funcionalidad.

Capacidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.	Cumple/no cumple. URL donde se describa funcionalidad.
Capacidad de identificar aplicaciones propietarias que usen los protocolos HTTP y TCP.	Cumple/no cumple. URL donde se describa funcionalidad.

Protección ante vulnerabilidades

Características mínimas requeridas	**Características ofertadas**
Capacidad de aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de/hacia Internet sin incurrir en latencia para no penalizar la experiencia de navegación del usuario. En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas. Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades especificando si son vulnerabilidades que aplican a los clientes, los servidores o a ambos indistintamente.	Cumple/no cumple. URL donde se describa funcionalidad.
Capacidad de categorizar las vulnerabilidades por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.	Cumple/no cumple. URL donde se describa funcionalidad.
Capacidad de usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.	Cumple/no cumple. URL donde se describa funcionalidad.

Filtrado de URL's

Características mínimas requeridas	**Características ofertadas**
Posibilidad de crear políticas basadas en control por URL'S y/o categorías de URL's para aplicarlas a la navegación http o https, permitiendo o bloqueando el acceso de los usuarios a determinadas páginas.	Cumple/no cumple URL donde se describa funcionalidad.
En caso de bloqueo, debe poder personalizarse la página mostrada al usuario, así como debe existir la posibilidad de solicitar la reclasificación de falsos positivos y negativos.	Cumple/no cumple. URL donde se describa funcionalidad.
Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.	Cumple/no cumple. URL donde se describa funcionalidad.

Antivirus

Características mínimas requeridas	Características ofertadas
Capacidad de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.	Cumple/no cumple. URL donde se describa funcionalidad.
Capacidad para aplicar las políticas de antivirus de forma granular, permitiendo, por ejemplo, la aplicación de dichas políticas a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.	Cumple/no cumple. URL donde se describa funcionalidad.

Tecnología de SandBoxing

Características mínimas requeridas	Características ofertadas
Posibilidad de disponer de un servicio en la nube para analizar ficheros de forma que se permita el envío de dicha información para análisis atendiendo a criterios como: • Tipo de aplicación que se está usando para transferir el fichero. • Tipo de fichero que se está transfiriendo. • Dirección de transferencia (descarga o subida de ficheros). Se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.	Cumple/no cumple. URL donde se describa funcionalidad.
Posibilidad de que el análisis realizado por este servicio en la nube, en caso de que la información enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad, deberá generar las firmas apropiadas en un plazo inferior a 10 minutos, que se utilizarán para actualizar los motores propios de antivirus, amenazas y filtrado URL, de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas.	Cumple/no cumple. URL donde se describa funcionalidad.

Bloqueo de ficheros y datos sensibles

Características mínimas requeridas	Características ofertadas
Capacidad de identificar ficheros no basándose en su extensión sino en el tipo MIME del archivo. Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de ficheros y se generen los logs correspondientes.	Cumple/no cumple. URL donde se describa funcionalidad.
También se requiere la capacidad de búsqueda de patrones sensibles como combinaciones de números de tarjetas de crédito de forma que se evite la filtración al exterior de este tipo de datos.	Cumple/no cumple. URL donde se describa funcionalidad.

Inspección SSL

Características mínimas requeridas	Características ofertadas
Capacidad de inspeccionar el tráfico SSL para analizar las comunicaciones y aplicar las funcionalidades de seguridad anteriores.	Cumple/no cumple. URL donde se describa funcionalidad.

Detección de equipos comprometidos en la red

Características mínimas requeridas	Características ofertadas
Capacidad de uso de motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con indicación de tiempos, usuarios, direcciones IP y vulnerabilidades o amenazas detectadas.	Cumple/no cumple. URL donde se describa funcionalidad.

Seguridad DNS

Características mínimas requeridas	Características ofertadas
Capacidad de habilitar mecanismos de DNS sinkholing que permitan interceptar las peticiones de resolución de nombre asociados a amenazas (botnets, malware, virus, etc..). Las firmas DNS deben permitir detectar técnicas de ocultación utilizadas por las amenazas como DGA/DNS tunneling aprovechando técnicas de análisis avanzado mediante machine learning con la información compartida por múltiples usuarios. Las firmas DNS se deberán crear y actualizar de forma automática.	Cumple/no cumple. URL donde se describa funcionalidad.
Para garantizar el adecuado nivel de protección de esta funcionalidad, al crecer exponencialmente el número de firmas DNS necesarias y no poder almacenarse localmente, deberá existir la posibilidad de realizar consultas en tiempo real de dominios contra un servicio en la nube del fabricante.	Cumple/no cumple. URL donde se describa funcionalidad.

Protección ante ataques de DDoS

Características mínimas requeridas	Características ofertadas
Capacidad de protección ante ataques de Denegación de Servicios de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las	Cumple/no cumple

direcciones IP origen y destino a inspeccionar o el usuario interno de la red que puede estar originando el ataque. Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.	

Informes

Características mínimas requeridas	**Características ofertadas**
Capacidad de generar informes tanto predefinidos como personalizados utilizando los logs. Los informes podrán generarse tanto manualmente como de forma automática y programada. También podrá agruparse varios informes en un único documento con formato PDF.	Cumple/no cumple

d) OTRAS CARACTERÍSTICAS

Virtual Systems

Características mínimas requeridas	**Características ofertadas**
Capacidad para la definición de instancias de firewall virtual en un mismo hardware físico. Cada instancia debe ser independiente, y gestionada de forma separada y el tráfico aislado del resto. Como mínimo se requieren 10 instancias.	Cumple/no cumple Indicar nº de instancias de firewall incluidas

Captura de tráfico

Características mínimas requeridas	**Características ofertadas**
Capacidad de realizar capturas del tráfico que atraviesa sus interfaces en formato PCAP, de forma que se puedan establecer filtros de captura basados en IP y puerto origen/destino, aplicación, etc.	Cumple/no cumple. URL donde se describa funcionalidad.

Geo-Localización

Características mínimas requeridas	**Características ofertadas**
Capacidad para la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.	Cumple/no cumple. URL donde se describa funcionalidad.
Capacidad de visualización de los países de origen y destino en la vista detallada de los logs de cualquier funcionalidad de seguridad.	Cumple/no cumple. URL donde se describa funcionalidad.

Integración con listas dinámicas de IPs de terceros

Características mínimas requeridas	**Características ofertadas**
Capacidad para descargar listas dinámicas de IPs de	Cumple/no cumple.

	terceros por comando o vía web (sin necesidad de hacer uso del API XML, tan solo indicando la URL de descarga), que se actualicen de manera automática, para incorporar inteligencia sobre orígenes o destinos maliciosos provenientes de otros servicios.	URL donde se describa funcionalidad.

e) CAPACIDAD Y RENDIMIENTO

No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, control de archivos, …). Se entiende por tanto que los rendimientos solicitados utilizan todas las firmas disponibles para cada mecanismo.

Descripción	Características mínimas requeridas	OFERTADO
Licencia Threat Prevention o similar	Sí (1 año)	
Threat prevention throughput	10 Gbps	
IPSec VPN throughput	11Gbps	
Nº máximo de sesiones soportadas	4.000.000	
Nuevas conexiones por segundo	180.000	

3. **Formación:**

Plan de formación: contenidos.

4. Garantía:

Características mínimas requeridas	Características ofertadas
Garantía 24x7 con reemplazo HW NBD	Cumple/no cumple

Anexo II. Descripción de las pruebas de validación técnica

La Fundación Integra realizará con el soporte técnico in-situ del licitador todas aquellas pruebas que considere necesarias para validar el cumplimiento de los requisitos mínimos y opcionales establecidos en la cláusula 9ª del presente pliego y, en particular, cualquiera de las descritas a continuación. Para la realización de las pruebas de validación técnica el equipo deberá ser idéntico al ofertado y tener todas las licencias de software necesarias para las funcionalidades que se contratan activadas.

A) Funcionalidades de seguridad. Para la realización estas pruebas el equipo deberá tener la suscripción de seguridad ThreadPrevention o similar ofertada activada, con todos los filtros y firmas disponibles. Toda la actividad será registrada en los logs para confirmar su eficacia y verificar cada una de las funcionalidades.

Prueba 1. Instalación en tap y redirección del tráfico mediante port-mirroring".

La prueba consistirá en la instalación en tap del equipo, que recibirá el tráfico real mediante "port-mirroring" de los usuarios de la Red CTnet, para que muestre sus capacidades y rendimiento. El volumen de tráfico a inyectar es aproximadamente de 8Gbps y 400.000 sesiones. En estas condiciones, se considerará apto el equipo únicamente si el uso de la CPU o cualquier otro parámetro interno no supera el 80%.

Prueba 2. Instalación en línea.

Si la prueba 1 es superada, el equipo se instalará en línea y recibirá el tráfico real directamente. El volumen de tráfico a inyectar es aproximadamente de 8Gbps y 400.000 sesiones.

En estas condiciones, y para garantizar el crecimiento futuro, se considerará apto el equipo únicamente si el uso de la CPU o cualquier otro parámetro interno no supera el 80%.

B) Integración con consola Panorama existente:

Prueba 1. Comprobación de que desde la consola Panorama se puede realizar la gestión de reglas de seguridad de forma simplificada para todos los tipos de políticas existentes en el equipo ofertado: firewall y Threat Prevention.

Prueba 2. Comprobación de que desde la consola Panorama se puede gestionar el proceso de actualización de software, licencias y contenido del equipo ofertado; esto incluye actualizaciones de aplicaciones, firmas de amenazas, etc.

Prueba 3. Comprobación de que desde la consola Panorama se puede extraer logs del equipo ofertado y almacenarlos localmente para la realización de consultas y elaboración de informes a partir de dichos logs

Superadas todas las pruebas, se considerará que el equipo cumple los requerimientos mínimos de funcionalidades exigidas.