SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

RENOVACIÓN, SOPORTE, MONITORIZACIÓN Y MANTENIMIENTO DEL EQUIPAMIENTO DE SEGURIDAD DE LA RED DE COMUNICACIONES DE LA UNIVERSIDAD DE ALCALÁ

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

INDICE

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

1. OBJETO DEL CONTRATO

El objeto de este contrato es la renovación de licencias y soporte de fabricante, la prestación de servicios profesionales de integrador para la monitorización y mantenimiento del equipamiento de seguridad de la Red de Comunicaciones de la Universidad de Alcalá (en adelante, UAH) y el suministro de nuevo equipamiento de seguridad para sustituir los equipos que quedan fuera de soporte.

2. SITUACIÓN ACTUAL DEL EQUIPAMIENTO DE SEGURIDAD

En la actualidad, los firewalls de red de la Red de Comunicaciones de la UAH son del fabricante FortiNet: en concreto los siguientes modelos, cada par en configuración HA Activo/Pasivo:

- 2 FortiGate 1000C, con los siguientes números de serie:
  - FGT1KC3911800230
  - FGT1K3912800976
- 2 FortiGate 1500D, con los siguientes números de serie:
  - FG1K5D3I15800311
  - FG1K5D3I15800400

Este equipamiento se complementa con un concentrador de logs FortiAnalyzer FAZVM64 con número de serie FAZ-VM0000041090 y con licencia para 25Gb de logs diarios.

Los firewalls cuentan con licenciamiento UTP (Unified Threat Prevention), que incluye IPS (Intrusion Prevention System), Protección Avanzada contra Malware, Control de Aplicaciones, Filtrado Web, Servicio Antispam y soporte 24x7 FortiCare. El FortiAnalyzer cuenta con soporte 24x7 FortiCare.

Los FortiGates 1500D tienen instalada la versión v5.6.8 build167, y los 1000C la v5.6.9 build1673.

El FortiAnalyzer tiene instalada la versión v6.4.4-build2253 201215.

Este licenciamiento y soporte de fabricante finaliza el 31 de diciembre de 2021. Igualmente, los equipos FortiGate 1000C finalizan su ciclo de vida (End of Support) en esa fecha.

Igualmente, el contrato de soporte actual por parte de integrador finaliza el 31 de diciembre de 2021.

La UAH cuenta además con un WAF (Web Application Firewall), también del fabricante FortiNet (este equipo no es objeto de este contrato).

Todo este equipamiento, mediante la funcionalidad Security Fabric, se conforma como una única entidad de seguridad con las siguientes características:

- Single Sign-On para Security Fabric: Posibilidad de autenticarse una única vez en el entorno de Firewalls de Security Fabric y que vía SAML se puedan compartir las credenciales de forma segura para no tener que re autenticar al administrador en el resto de los Firewalls o en la plataforma de logs y reporting.
- Visibilidad completa del entorno de Firewalls: Capacidad para unificar en un panel toda la visibilidad de la red de cortafuegos, recogiendo tanto la topología física como lógica. Esto permite ubicar de forma rápida los elementos más críticos de la red, como aquellos servidores que contienen información más sensible, desde un panel único dentro de Security Fabric
- Analítica de seguridad en un panel único: Posibilidad de mostrar los principales logs y analítica de seguridad en el Firewall principal de la red, aunque la información resida en el gestor de logs, eventos e informes de Security Fabric.
- Integración con políticas de seguridad de protección en puesto: El entorno colaborativo Security Fabric facilita que sólo aquellos PCs que cumplan las normativas y políticas de puesto, puedan atravesar la capa de cortafuegos. Incluso existe la posibilidad de establecer dichas políticas por perfiles en la primera capa de Firewall del entorno, haciendo que el tráfico no fluya por la red si no se cumplen las premisas de seguridad de puesto básicas. Esto se podrá realizar desde una consola centralizada de gestión de la solución de Endpoint del mismo fabricante para ofrecer visibilidad, así como gestionar y asignar los perfiles de seguridad en puesto

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- Integración con WAF: Posibilidad de intercambio de información entre los cortafuegos y el dispositivo WAF del mismo fabricante para reconocer ataques de manera temprana contra los servicios web del entorno protegido por Security Fabric.

De igual manera, los firewalls tienen implementadas funcionalidades SSO (Single Sign On) para la validación de reglas con control de acceso por usuario, para usuarios de dominio, mediante agentes Fortinet Single Sign On para Windows AD instalados en dos máquinas virtuales.

La UAH tiene implementado segundo factor de autenticación para el acceso por VPN SSL mediante FortiTokens.

Los cambios de ubicación o de versión del software del equipamiento anterior no´supondrán gasto alguno para la UAH.

3. PRESTACIONES Y SERVICIOS A REALIZAR

Las prestaciones y servicios que se deben realizar para conseguir el objeto de este contrato son los siguientes.

3.1 Gestor único del servicio

El adjudicatario designará en el plazo de quince días desde el día siguiente de la firma del contrato un Gestor del Servicio, encargado de la puesta en marcha, supervisión, coordinación y control del servicio, siendo el interlocutor único para los asuntos derivados de la gestión del servicio.

El Gestor único del servicio se encargará, al menos, de:

- Definir un modelo de procesos, personalizado y aprobado por el Servicio de Comunicaciones de la UAH, para la prestación de los servicios objeto del contrato al inicio de la ejecución del contrato, en el plazo máximo de un mes desde la firma. Los procesos por modelar serán al menos los siguientes:
  - Gestión de incidencias y solicitudes.
  - Protocolo de escalado.
  - Control de la ejecución del contrato.
  - Procedimientos y procesos relacionados con la monitorización 24x7.
  - Procedimientos y procesos del mantenimiento preventivo, correctivo y adaptativo.

  Cada proceso definirá como mínimos los siguientes aspectos: procedimiento, actividades del proceso, roles y responsabilidades, entregables y herramientas de soporte a los procesos.
- La puesta en marcha de los servicios relacionados con el Centro de Gestión de Incidencias y la monitorización 24x7.
- La elaboración de los informes definidos en el apartado 5.3. Igualmente, a requerimientos de los responsables del Servicio de Comunicaciones de la UAH, deberá generar los informes que le sean solicitados.

3.2 Centro de Gestión de Incidencias

Se dispondrá de un punto de contacto con el adjudicatario para la atención de solicitudes e incidencias, que tramitará las peticiones realizadas por el personal de los Servicios Informáticos.

El canal de contacto será al menos por e-mail y por teléfono, con una cobertura mínima 12x5 (desde el lunes al viernes y de 8:00 a 20:00 horas) y un tiempo de respuesta máximo mediante el acuerdo de nivel de servicio, para la comunicación de incidencias y peticiones.

La supervisión, coordinación y control del servicio será realizado por el Gestor del Servicio designado por el adjudicatario.

El adjudicatario habilitará igualmente un canal 24x7x365 para la comunicación de incidencias críticas.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

3.3 Monitorización 24x7

El adjudicatario monitorizará el equipamiento crítico descrito en el apartado 5.1, con el envío de alarmas y alta de incidencias ante fallos y umbrales superados, pudiendo utilizar su propio software de monitorización o el ya existente en la UAH.

Esta monitorización se realiza sobre equipamiento crítico de la red de comunicaciones, por lo que el integrador deberá actuar y resolver cualquier incidencia que pudiera ocurrir en ellos en horario 24x7x365, tanto de forma remota como on-site, según el acuerdo de nivel de servicio en el apartado 5.2.

En el caso de que el adjudicatario utilice sus propios medios para la monitorización, deberá tener en cuenta lo siguiente:

- El integrador deberá proporcionar el equipamiento necesario para establecer una conexión segura IPSec en caso de que quiera monitorizar el equipamiento de la UAH desde su NOC, o bien establecer un túnel IPSec contra el terminador de túneles corporativo (FortiGate 1500D).
- Si se requiere la instalación del software de monitorización en la red de la UAH, o cualquier otro servidor de soporte, se optará por su despliegue en entorno virtualizado VMWare. El integrador será el responsable de proporcionar el fichero ".ova" de la máquina virtual, y se hará cargo de todas las licencias necesarias para el funcionamiento del software de monitorización durante el periodo del contrato y las posibles prórrogas, incluidas las licencias del sistema operativo. Así mismo, deberá cumplir con la política de bastionado y securización de servidores de la UAH.

El Servicio de Comunicaciones de la UAH proporcionará acceso mediante cliente FortiClient VPN SSL para los técnicos de soporte con doble factor de autenticación mediante FortiToken Mobile.

En caso de que el integrador detecte una incidencia que, afectando a la red de comunicaciones, no sea objeto de este contrato, deberá escalarla a otros soportes de la infraestructura de comunicaciones.

Toda la información que recabe el sistema de monitorización será propiedad de la UAH. A petición de la UAH, esta información deberá ponerse a su disposición en el plazo de 15 días en un formato abierto a acordar entre el Gestor del Servicio y los SSII.

La monitorización del equipamiento crítico de red deberá estar operativa en un plazo máximo de dos meses desde el día siguiente al de la firma del contrato.

3.4 Mantenimiento preventivo, correctivo y adaptativo

El adjudicatario realizará el mantenimiento preventivo, correctivo y adaptativo de las dos unidades FortiGate 1500D y del FortiAnalyzer, debiendo realizar al menos las siguientes acciones:

- Realizar, en el plazo máximo de tres meses, una auditoria sobre el estado del equipamiento objeto de este contrato. Como consecuencia de esta auditoría, se elaborará un informe con las conclusiones obtenidas y el plan de actuación en caso de detectar incidencias o anomalías graves. La auditoría contendrá al menos información de:
    - Versiones de software del equipamiento.
    - Estado de las configuraciones.
    - Estado del equipamiento, CPU, memoria, ventiladores, fuentes de alimentación, etc.
    - Uso de puertos, tanto de usuario como de uplink-downlink.
    - Errores en los equipos.

  Esta auditoría se realizará anualmente durante la duración del contrato.
- Realizar, en el plazo máximo de tres meses, una auditoría de seguridad y conformidad con las recomendaciones del CCN-CERT y de la propia UAH sobre el equipamiento de seguridad objeto

de este contrato. Como consecuencia de esta auditoría, se elaborará un informe con las conclusiones obtenidas y el plan de actuación de acciones correctivas en caso de detectar incidencias o anomalías graves. Esta auditoría se realizará anualmente durante la duración del contrato.

- Renovación de la licencia UTP y soporte 24x7 FortiCare para los dos FortiGates 1500D, con una duración de 3 años, a partir de la fecha de fin de soporte del fabricante (31 de diciembre de 2021).
- Renovación de la licencia de 25Gb de logs diarios y el soporte 24x7 FortiCare para el FortiAnalyzer, a partir de la fecha de fin de soporte del fabricante (31 de diciembre de 2021).
- Soporte N2 y resolución de incidencias, apertura y gestión de tickets de soporte con el fabricante.
- Gestión de la garantía del equipamiento y del soporte del fabricante, con recogida en las dependencias de la UAH del equipamiento averiado, gestión del reemplazo y devolución del equipo nuevo a la UAH. Todo este proceso debe ser asumido por el adjudicatario sin coste alguno para la UAH.
- En caso de elementos obsoletos o llegados a su end-of-life, se podrá optar por la sustitución del elemento por otro de equivalentes funcionalidades y prestaciones, manteniendo la homogeneidad de la red y la interoperabilidad completa con el resto de los elementos.
- El adjudicatario proporcionará usuarios de acceso a los portales Knowledge Base y FortiCloud para los técnicos del área de Comunicaciones de los Servicios Informáticos, así como a las listas de distribución de información técnica del fabricante.
- Actualizaciones de software. Estas actualizaciones se deberán realizar al menos una vez al año durante la duración del contrato, siempre y cuando exista una versión estable disponible de los fabricantes, o por recomendación de los soportes de los fabricantes.
    - Las actuaciones que deba realizar el adjudicatario sobre el equipamiento de red, tanto hardware y software objeto de este contrato, tanto si son como respuesta a incidencias detectadas en la monitorización 24x7, o como consecuencia de incidencias o peticiones comunicadas por el Servicio de Comunicaciones, se realizarán teniendo en cuenta el principio de minimización de impacto. Esto es, preferentemente fuera del horario de 8:00 a 20:00 horas y de forma remota siempre que sea posible.
- Las actuaciones relacionadas con el mantenimiento y soporte del equipamiento de red, tanto hardware como software, podrán realizarse tanto de forma remota como presencial, estas últimas sin coste adicional alguno para la UAH.

El adjudicatario comenzará a prestar este servicio para el equipamiento FortiGate 1500D y FortiAnalyzer a partir de 1 de enero de 2022.

Los plazos indicados comenzarán a partir del día siguiente de la firma del contrato.

3.5 Suministro de Firewalls NGFW para renovación tecnológica

Los dos equipos FortiGate 1000D finalizan su vida útil el 31 de diciembre de 2021, por lo que es necesario adquirir nuevo equipamiento de seguridad que los sustituya.

Este nuevo equipamiento permitirá además adaptarse a la evolución tecnológica de los nuevos enlaces de datos de la UAH con el proveedor de servicios de Internet RediMadrid, entidad que gestiona la red de alta velocidad de investigación y educativa de la Comunidad de Madrid, que prevé ampliar la velocidad de acceso a 100Gb.

Deberá ser completamente compatible, interoperable y funcional con el equipamiento de seguridad hardware y software descritos en este pliego, incluyendo las funcionalidades Security Fabric, SSO y FortiToken.

Se deben suministrar dos Firewalls NGFW en configuración HA Activo-Pasivo. Cada equipo deberá tener las siguientes características técnicas generales:

- Interfaces de conexión:
    - 4 interfaces 100 GE QSFP28 / 40 GE QSFP+
    - 24 interfaces 25 GE SFP28 / 10 GE SFP+ / GE SFP

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- Rendimiento del sistema
  - Throughput IPS (con logging habilitado) -> 44 Gbps
  - Throughput NGFW (con IPS y Control de Aplicaciones habilitado) -> 34 Gbps
  - Throughput Protección ante Amenazas (con IPS, Control de Aplicaciones, Filtrado de URLs y Protección contra Malware habilitado) -> 25 Gbps
  - Throughput del Firewall (para paquetes de 1518 / 512/ 64 bytes y UDP) -> 240 / 238 / 150 Gbps
  - Throughput del Firewall en paquetes por segundo -> 225 Mpps
  - Sesiones TCP concurrentes -> 50 Millones
  - Nuevas sesiones TCP por segundo -> 850.000
  - Throughput VPN-SSL -> 11 Gbps
  - Usuarios concurrentes VPN-SSL en modo túnel -> 30.000
  - Throughput inspección SSL para IPS -> 30 Gbps
  - Sesiones concurrentes para inspección SSL IPS -> 4.9 Millones
  - Throughput Control de Aplicaciones, para HTTP de 64k -> 86 Gbps

Los equipos deben suministrarse con doble fuente de alimentación redundante AC, y con los kits correspondientes para su montaje en rack.

El suministro y puesta en marcha de los dos nuevos firewalls NGFW se realizará en un plazo máximo de dos meses a partir del día siguiente al de firma del contrato.

Además, deben suministrarse las licencias correspondientes para las siguientes funcionalidades para un periodo de 3 años:

- Soporte del fabricante 24x7
- Servicios Next Generation Firewall:
  - Control de Aplicaciones
  - IPS
  - Protección Avanzada contra Malware y Antivirus
  - Filtrado Web
  - Antispam

Este equipamiento deberá considerarse como equipamiento crítico de prioridad 1 en cuanto Acuerdo de Nivel de Servicio, e incluirse en la prestación de servicios de soporte, mantenimiento y monitorización.

La fecha de prestación de los servicios de integrador y del soporte y licencias del fabricante correspondientes tendrán una duración de 3 años, a contar desde su suministro.

Además, el adjudicatario deberá encargarse de su instalación y configuración según las directrices de los Servicios Informáticos de la UAH.

En el punto 6.1 de este documento se especifican el resto de las características técnicas y funcionalidades mínimas que debe cumplir este equipamiento a suministrar.

Para el correcto conexionado de este equipamiento a la Red de Comunicaciones de la UAH se requiere igualmente del suministro de los siguientes transceptores ópticos certificados por el fabricante del equipamiento anterior:

- 4 transceptores ópticos de 100 GE (QSFP28), para fibra óptica multimodo OM4 y longitud de onda 850 nm, con longitud de enlace máxima de 100 metros.

En el punto 6.2 de este documento se especifican el resto de las características técnicas y funcionalidades mínimas que debe cumplir estos transceptores ópticos.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

3.6 Suministro de una consola de administración centralizada de los endpoints conectados por VPN SSL

Debido al aumento progresivo del teletrabajo y de las conexiones por VPN SSL, se requiere el suministro de una consola de administración centralizada de los clientes VPN SSL corporativos, licenciada para 500 usuarios durante 3 años.

Las principales características que debe tener este sistema son:

- Interfaz gráfico para gestión del sistema
- Dashboard en tiempo real
- Despliegue remoto de clientes VPN en los endpoints
- Gestión del inventario de software
- Integración con Directorio Activo
- Gestión central de cuarentenas
- Asignación automática de grupos de usuarios
- Control dinámico de acceso
- Automatización de envío de correos electrónicos de alertas.
- Soporte de grupos customizados
- Disparadores remotos

Esta consola se proporcionará en formato Virtual Machine, y se desplegará en la infraestructura de virtualización existente en la UAH.

Todo el sistema deberá contar con soporte de fabricante 24x7 y licenciamiento válido durante la duración del contrato y se considerará incluido en la prestación de servicios de soporte y mantenimiento.

El adjudicatario deberá encargarse de su instalación y configuración según las indicaciones de los Servicios Informáticos de la UAH.

Los clientes VPN licenciados deberán tener las siguientes características:

- Disponible para los siguientes sistemas operativos:
  - Windows.
  - MAC OS X
  - Android
  - iOS
  - Linux
- VPN SSL
- Antivirus
- Detección de amenazas basada en servicios cloud
- Filtrado Web
- Firewall de Aplicación

Tanto la consola de gestión como los clientes VPN deberán ser completamente compatibles, interoperables y funcionales con el equipamiento de seguridad hardware y software descritos en este pliego, incluyendo las funcionalidades Security Fabric y FortiToken.

En el punto 6.3 de este documento se especifican el resto de las características técnicas y funcionalidades mínimas que debe cumplir este equipamiento a suministrar.

3.7 Servicios profesionales

El adjudicatario pondrá a disposición de la UAH una bolsa de 30 horas anuales por cada año de duración del contrato o parte proporcional, de servicios profesionales de consultoría, asesoramiento y configuración, para el despliegue de nuevas funcionalidades, configuraciones, etc., aplicables a todo el equipamiento objeto del contrato.

3.8 Transferencia tecnológica

Para asegurar el correcto uso de la consola de administración centralizada de *endpoints*, de forma gratuita, proporcionará al menos una sesión de transferencia de información para 8 técnicos de los Servicios Informáticos, que tendrá lugar en dependencias de la UAH. La sesión será impartida por formadores certificados por el fabricante o por el mayorista del equipamiento y con experiencia en dicha consola.

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar en todo momento a las personas designadas por la UAH a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

4. SEGUIMIENTO, CONTROL Y SUPERVISIÓN DE LA EJECUCIÓN

Las actividades que se realizarán para el seguimiento, supervisión y control de la ejecución del contrato son las siguientes:

- Nombrar un Gestor único del servicio por parte del adjudicatario en el plazo de quince días.
- Entrega en el plazo de quince días de la certificación FortiNet NS4 activa al menos para técnico de soporte asignado al mismo, y el certificado como al menos Advanced Partner del adjudicatario por parte del fabricante FortiNet, así como la certificación necesaria que habilite al adjudicatario como soporte e integrador autorizado de cualquier solución propuesta.
- Definición en un plazo de un mes por parte del Gestor del servicio de un modelo de procesos, personalizado y aprobado por el Servicio de Comunicaciones con la UAH, para la prestación de los servicios objeto del contrato.
- Contratación del soporte de los distintos fabricantes en el plazo máximo de un mes, con la presentación del consiguiente documento acreditativo.
- Suministro y puesta en marcha del equipamiento para renovación tecnológica en el plazo de dos meses.
- Suministro y puesta en marcha de la consola de administración centralizada del endpoint en el plazo de dos meses.
- Puesta en marcha en el plazo máximo de dos meses de la monitorización 24x7.
- Prestación de los servicios de soporte de integrador (soporte, mantenimiento y monitorización) para el equipamiento FortiGate 1500D y FortiAnalyzer a partir del 1 de enero de 2022.
- Prestación de los servicios de integrador (soporte, mantenimiento y monitorización) para el equipamiento de renovación tecnológica y la consola de administración centralizada y las licencias de cliente VPN SSL a partir de su suministro, por una duración de 3 años.
- Auditorias del estado del equipamiento hardware y software, y cumplimiento del ENS, de la red de comunicaciones objeto de este contrato, el plazo máximo de tres meses, que se repetirá anualmente.
- Proporcionar al Servicio de Comunicaciones de la UAH, en el plazo máximo de 3 meses de usuarios de acceso a los portales de conocimiento y documentación de los fabricantes.
- Sesiones de transferencia tecnológica sobre la consola de administración centralizada del endpoint en el plazo máximo de 2 meses.

Todos los plazos indicados comenzarán a partir del día siguiente de la firma del contrato.

5. MONITORIZACIÓN 24x7 Y ACUERDO DE NIVEL DE SERVICIO

5.1 Monitorización 24x7

Los elementos críticos de la red deberán estar monitorizados mediante herramientas automáticas de forma continua, con envío de alarmas y alta de incidencias ante fallos y por umbrales superados.

El equipamiento crítico que debe ser objeto de la monitorización 24x7 es el siguiente:

- Las dos unidades FortiGate 1500D
- Los dos Firewalls NGFW suministrados como renovación tecnológica.

5.2 Acuerdo de Nivel de Servicio

La resolución de incidencias, tanto en remoto como on-site, se realizará en cobertura 24x7 para los elementos de prioridad 1 y en cobertura 12x5 (lunes a viernes de 8:00 a 20:00) para los de prioridad 2 y 3. La prioridad se establece en función del impacto y la urgencia de cada elemento de red cuando funciona incorrectamente. A continuación, se detalla la prioridad del equipamiento de red:

- PRIORIDAD 1 (ALTA):
  - 2 unidades FortiGate 1500D
  - 2 unidades NGFW renovación tecnológica
- PRIORIDAD 2 (MEDIA):
  - Consola de administración centralizada del endpoint
- PRIORIDAD 3 (BAJA):
  - FortiAnalyzer

El cumplimiento de los requisitos especificados dentro del presente pliego se regulará por un “Acuerdo de Nivel de Servicio” (ANS). En consecuencia, las tareas correspondientes deberán realizarse ajustándose a los “Indicadores de nivel de servicio (INS)” y “valores objetivos” (VO) detallados a continuación.

Estos INS y VO tienen carácter de mínimos. El adjudicatario se comprometerá a ampliar los indicadores que la UAH le solicite durante la ejecución del contrato y a establecer de común acuerdo VO para todos ellos.

El adjudicatario, dentro del ámbito de las prestaciones que se regulen por el sistema de ANS, será responsable del cumplimiento de todos los VO establecidos, con independencia de los recursos que para ello tenga que incorporar en cada momento. Así mismo, si existen acuerdos de servicio firmados con sus proveedores de mantenimiento y soporte, previamente autorizados por la UAH, éstos respaldarán los niveles de servicio acordados.

La descripción de categorización de las incidencias es la que sigue a continuación:

1) **Críticas:** Incidencias en equipos con **PRIORIDAD 1.**
2) **Urgentes:** Incidencias en equipos con **PRIORIDAD 2.**
3) **Ordinarias:** Incidencias en equipos con **PRIORIDAD 3.**
4) **Leves.** El resto de las peticiones y servicios no pertenecientes a otras categorías.

Los indicadores contemplados para este servicio son los siguientes:

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

1.- Tiempo de respuesta: Plazo máximo transcurrido desde el momento que la incidencia es detectada o comunicada al adjudicatario y registrada en el sistema de gestión de incidencias y peticiones, hasta que los técnicos de la empresa adjudicataria comienzan a trabajar en la incidencia.

Indicador	Valor objetivo	Valor mínimo de cumplimiento
Plazo máximo de atención en la categoría Crítica	<=2 horas	95%
Plazo máximo de atención en la categoría Urgente	<=4 horas	95%
Plazo máximo de atención en la categoría Ordinaria	<=8 horas	95%
Plazo máximo de atención en la categoría Leve	<=48 horas	95%

Los valores serán contabilizados en los horarios indicados para la cobertura 12x5 o 24x7 según la criticidad del equipamiento. Los valores contabilizados serán los no achacables a la lógica de los propios sistemas de gestión o bien a errores o falta del software base para los que no exista solución conocida en forma de parche o procedimiento documentado.

2.- Tiempo de resolución: Plazo máximo transcurrido desde el momento que la incidencia es detectada o comunicada al adjudicatario y registrada en el sistema de gestión de incidencias y peticiones, hasta que la misma queda resuelta y con el visto bueno de los Servicios Informáticos. Los indicadores que se deben tener en cuenta son:

Indicador	Valor objetivo	Valor mínimo de cumplimiento
Plazo máximo de resolución en la categoría Crítica	<=8 horas	95%
Plazo máximo de resolución en la categoría Urgente	<=24 horas	95%
Plazo máximo de resolución en la categoría Ordinaria	<=48 horas	95%
Plazo máximo de resolución en la categoría Leve	<=7 días	95%

Los valores serán contabilizados en los horarios indicados para la cobertura 12x5 o 24x7 según la criticidad del equipamiento**.** Los valores contabilizados serán los no achacables a la lógica de los propios sistemas de gestión o bien a errores o falla del software base para los que no exista solución conocida en forma de parche o procedimiento documentado.

5.3 Informes de seguimiento

El Gestor del servicio presentará al Servicio de Comunicaciones de la UAH un informe trimestral de las incidencias y estado de los servicios asociados a este contrato.

El informe contendrá la información detallada y la agrupada del último trimestre, incluyendo, al menos:

- Resumen de los incidentes registrados durante el trimestre.
    - Incidentes por prioridad de equipo.
    - Alarmas por superación de umbral en los parámetros y equipos definidos por los SSII.
    - Informe sobre la intervención de los técnicos de campo indicando, al menos:
        - N.º de aviso
        - Fecha y hora de la intervención
        - Descripción, en la que indicará el equipo afectado y el motivo de la intervención

        - Fecha fin de avería
        - Solución, donde se indicará la solución proporcionada
        - Técnico de campo que realiza la intervención
    - En todos los informes se especificarán la dirección IP y el nombre de los equipos monitorizados.
- Servicios profesionales
    - Horas consumidas, con indicación del técnico asociado y agrupadas por consulta o petición.
    - Horas remanentes.

6. CARACTERÍSTICAS TÉCNICAS DEL EQUIPAMIENTO A SUMINISTRAR

6.1 Firewalls NGFW para renovación tecnológica

Las características técnicas de los Firewalls NGFW son las siguientes:

- Interfaces
    - Puertos 100 GE QSFP28 / 40 GE QSFP+ -> 4
    - Puertos 25 GE SFP28 / 10 GE SFP+ / GE SFP -> 24
    - Puertos de gestión GE RJ45 -> 2
    - Puertos USB (Cliente/Servidor) -> 1/1
    - Puerto de consola -> 1
- Rendimiento del sistema para mezcla de tráfico Enterprise
    - Throughput IPS (con logging habilitado) -> 44 Gbps
    - Throughput NGFW (con IPS y Control de Aplicaciones habilitado) -> 34 Gbps
    - Throughput Protección ante Amenazas (con IPS, Control de Aplicaciones, Filtrado de URLs y Protección contra Malware habilitado) -> 25 Gbps
- Rendimiento del sistema y capacidad
    - Throughput del Firewall (1518 / 512 / 64 bytes, UDP) -> 240 /238 /150 Gbps
    - Throughput Firewall IPv6 (1518 / 512 / 86 bytes, UDP) -> 240 /238 / 150 Gbps
    - Latencia del Firewall (64 bytes, UDP) -> 3.33 µs
    - Throughput del Firewall en paquetes por segundo -> 225 Mps
    - Sesiones TCP concurrentes -> 50 Millones
    - Nuevas sesiones TCP por segundo -> 850.000
    - Políticas de Firewall -> 200.000
    - Throughput IPSec VPN (512 bytes) -> 140 Gbps
    - Túneles IPSec VPN gateway-to-gateway -> 40.000
    - Túneles IPSec VPN client-to-gateway -> 200.000
    - Throughput SSL VPN -> 11 Gbps
    - Usuarios concurrentes SSL VPN modo túnel máximo recomendado -> 30.000
    - Throughput inspección SSL para IPS -> 30 Gbps
    - Sesiones concurrentes para inspección SSL IPS -> 4.9 Millones
    - Throughput Control de Aplicaciones, para HTTP de 64k -> 86 Gbps
    - Dominios virtuales (por defecto/máximo) -> 10/500
    - Opciones de configuración HA -> Activo/Activo, Activo/Pasivo, Clúster
- Certificaciones
    - ICSA Labs: Firewall, IPSec, Network IPS, Anti-Malware, SSL-TLS, Advanced Threat Defense, Web Application Firewalls; NSS Labs y Common Criteria
- Cumplimiento
    - FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- Consumo energético, ruido y especificaciones ambientales de funcionamiento
    - Potencia consumida (media/máxima) -> 513W / 738W
    - Disipación de calor -> 2484 BTU/h
    - Fuente de alimentación redundante e intercambiable en caliente
    - Nivel de ruido -> 63 dBA
- Funcionalidades y características avanzadas

  - Capacidad de configuración de proxy explícito por interfaz.
  - Visualización de número de usos y cantidad de tráfico de cada regla, así como de la última vez que se ha utilizado.
  - Funcionalidades integradas de IPS, Antimalware (en modo flujo o en modo proxy), Antispam y filtrado de contenidos o categorías web. No se acepta ningún acuerdo OEM con terceros, es decir, todas estas funcionalidades tienen que ser del propio fabricante de seguridad.
  - Funcionalidad Anti DoS, permitiendo definir políticas DoS por interfaz, origen, destino y protocolo.
  - Licenciamiento de funcionalidades por equipo, no por usuario.
- Control de aplicaciones
  - Clasificación de las aplicaciones en diferentes categorías y subcategorías.
  - Uso de la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red.
  - Aplicación de técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
  - Creación de firmas personalizadas de IPS y control de aplicaciones.
  - Capacidad para identificar las aplicaciones bajo túneles HTTPS.
- Identificación de usuarios
  - Integración con Microsoft Active Directory y Novel eDirectory para la identificación de usuarios.
  - Soporte de mensajes Radius Accounting para Single Sign On.
  - Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+.
  - Generación de usuarios de tipo invitado con tiempo de caducidad configurable (desde la creación o primera sesión).
  - Acceso de usuarios invitados mediante GUI sencilla y sin permisos de acceso a ningún otro parámetro de la gestión del firewall.
- Visibilidad
  - Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, web sites y aplicaciones cloud) para su visualización.
  - Visualización “Drill-down”.
- Filtrado de contenidos
  - Monitorización y control de la navegación web sin penalizar el tiempo de respuesta ni la experiencia del usuario.
  - Toma de decisiones en tiempo real, como permitir / denegar una URL basándose en políticas y en una base de datos de URLs mundiales, permitiendo establecer controles para un filtrado granular de las URLs.
  - El filtrado URL debe tener la funcionalidad de aplicar cuotas de tiempo para aquellas categorías deseadas. También ha de permitir crear categorías personalizables como listas blancas/negras.
  - Capacidad de filtrado basado en las peticiones DNS y las categorías URL, así como realización de sinkhole.
- Seguridad
  - Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.
  - Capacidad para definir múltiples reglas de seguridad en las interfaces origen / destino, incluyendo "fecha".
  - Modos de funcionamiento:
    - Modo transparente.
    - Modo router y / o modo sniffer.
  - Prevención de amenazas en tiempo real, detectando un amplio abanico de malware y exploits de vulnerabilidades (virus, spyware, gusanos, etc) sin incurrir en latencia, tanto en modo flow, como en modo proxy.
  - Funcionamiento como IPS basado tanto en patrones como en “Rated based”.
  - Posibilidad de crear firmas de IPS customizadas.
  - Descarga y aplicación automática de actualizaciones de las firmas antivirus, antispyware, base de datos de URLs, firmas IPS y de las nuevas aplicaciones identificadas.

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

- Funcionalidad integrada de doble factor de autenticación vía token hardware o software en dispositivo móvil, así como por SMS, integrado en la misma plataforma de seguridad, compatible con FortiToken.
- Funcionalidad de reconocimiento del tipo de dispositivo del cliente (IPhone, IPad, Android, etc ...) y poder hacer políticas en función del tipo de dispositivo, sin la instalación de ningún agente en el dispositivo remoto.
- Soporte para tráfico VoIP: SIP/H.323 /SCCP NAT trasversal, RTP
- Soporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Definición de objetos para aplicación en políticas de seguridad, de diferentes tipos: IP, Subnet, intervalo de IPs, geográficos y FQDN
- Detección y bloqueo de botnets en base a listas de reputación globales.
- Inspección de tráfico cifrado SSL mediante rotura de túnel SSL y mediante inspección de certificados.
- Posibilidad de integración con sistema de Sandboxing para detección de amenazas avanzadas mediante un equipamiento adicional físico o virtual (este equipamiento adicional no es objeto de la presente licitación) así como posibilidad de integración con un sistema de Sandboxing en la nube mediante licencias adicionales (estas licencias no son objeto de la presente licitación).
- Motor WAF (Web Application Firewall) integrado para proteger portales Web de ataques genéricos.

- Prevención de fuga de datos
  - Capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como asociaciones concretas
  - Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de archivo, diccionario y plantillas corporativas.
  - Detección e identificación de documentos mediante "Fingerprint".
  - Posibilidad de añadir marcas de agua en los documentos de Office.
- VPN
  - El sistema propuesto deberá cumplir los estándares de la industria, sin el apoyo externo de hardware o módulos adicionales:
    - IPSEC VPN
    - PPTP VPN
    - L2TP VPN
    - SSL VPN
  - Poder crear arquitecturas de creación dinámica de VPN site-to-site mediante estándar ADVPN.
  - El sistema propuesto deberá soportar 2 modos de funcionamiento SSL VPN:
    - Sin cliente - Acceso web: para clientes remotos que sólo necesitan un navegador y no requiere la instalación de ningún software, a fin de acceder vía web en: HTTP / HTTPS Proxy, FTP, Telnet, SMB / CIFS, SSH, VNC y RDP. El acceso RDP tiene que ser vía HTML, no con tecnología Java.
    - Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor.
  - Integración con la consola de administración centralizada del endpoint.
- Alta disponibilidad
  - Failover Activo / Pasivo, Activo / Activo y clustering sin necesidad de licencia.
  - Capacidad de virtual clustering con los dominios virtuales. Esta capacidad tiene que permitir configurar el nodo master de diferentes dominios virtuales de forma cruzada dentro del mismo clúster.
  - Sincronización de configuración y sesiones.
  - Interfaces reservados para gestión.
  - Posibilidad de configurar interfaces HeartBeat redundantes.
  - Reposición automática del Servicio:
    - Monitorización de interfaces (locales y remotos).
    - Sin pérdida de sesiones.
    - Conmutación en menos de 1 segundo.
  - Diferentes opciones de arquitectura:

SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

        - HA con agregación de enlaces.
        - Full mesh HA.
        - Soporte de clúster geográfico (equipos en distinta ubicación física).
- Networking
    - Soporte de protocolos RIP v1 y v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6.
    - Routing basado en políticas.
    - Soporte Dual Stack IPv4 e IPv6 simultáneo.
    - Network address translation NAT IPv4, NAT64 y NAT66.
    - DHCP server / DHCP Relay
    - DNS Server y DNS Proxy
    - NTP Server
    - 802.1Q VLANs
    - Routing basado en contenidos: ICAP y WCCP
    - Point-to-Point Protocol over Ethernet (PPPoE).
    - 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.
    - Capacidad de funcionalidad de VXLAN sobre túneles IPSec.
    - Servicio de DDNS integrado en el equipo para más de una interface.
- Balanceo de servidores
    - Funcionalidad de asociación y balanceo de servidores.
- Certificados
    - Funcionalidad de ssl off-loading
- Gestión y administración
    - Soporte de SNMP.
    - Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente en máquina externa al firewall para su administración y / o cualquier otra función del firewall.
    - Creación de diferentes cuentas de administración con diferentes niveles de acceso.
    - Aplicación de cambios de forma inmediata, sin ninguna espera en su aplicación.
    - Compatibilidad de sFlow y Netflow.
- Balanceo de tráfico hacia Internet
    - El sistema debe ser capaz de realizar balanceo de carga de los enlaces de Internet de forma dinámica con métodos opcionales de:
        - Por volumen.
        - Por sesiones.
        - Por IP de origen.
        - Por IP de origen + IP destino.
        - Spill-over (también llamada basada en el uso).
        - Según la calidad de la línea de internet, utilizando la latencia y jitter (de forma dinámica).
    - El sistema debe ser capaz de proporcionar redundancia de enlaces WAN monitorizando el estado de las líneas.
    - También se debe poder balancear el tráfico de salida en función del servicio utilizado en internet. Para ello el equipo deberá contener una base de datos predefinida con las aplicaciones de internet identificadas por sus IP públicas, Protocolos y puertos.
- Integración con Security Fabric
    - Single Sign-On para Security Fabric: Posibilidad de autenticarse una única vez en el entorno de Firewalls de Security Fabric y que vía SAML se puedan compartir las credenciales de forma segura para no tener que re autenticar al administrador en el resto de los Firewalls o en la plataforma de logs y reporting.
    - Visibilidad completa del entorno de Firewalls: Capacidad para unificar en un panel toda la visibilidad de la red de cortafuegos, recogiendo tanto la topología física como lógica. Esto permite ubicar de forma rápida los elementos más críticos de la red, como aquellos servidores que contienen información más sensible, desde un panel único dentro de Security Fabric.
    - Analítica de seguridad en un panel único: Posibilidad de mostrar los principales logs y analítica de seguridad en el Firewall principal de la red, aunque la información resida en el gestor de logs, eventos e informes de Security Fabric

- Integración con políticas de seguridad de protección en puesto: El entorno colaborativo Security Fabric facilita que sólo aquellos PCs que cumplan las normativas y políticas de puesto, puedan atravesar la capa de cortafuegos. Incluso existe la posibilidad de establecer dichas políticas por perfiles en la primera capa de Firewall del entorno, haciendo que el tráfico no fluya por la red si no se cumplen las premisas de seguridad de puesto básicas. Esto se podrá realizar desde una consola centralizada de gestión de la solución de Endpoint del mismo fabricante para ofrecer visibilidad, así como gestionar y asignar los perfiles de seguridad en puesto.
- Integración con WAF: Posibilidad de intercambio de información entre los cortafuegos y el dispositivo WAF del mismo fabricante para reconocer ataques de manera temprana contra los servicios web del entorno protegido por Security Fabric.

6.2 Transceptores ópticos 100 GE QSFP28

Las características técnicas de los transceptores ópticos 100 GE QSFP28 son las siguientes:

- Transceptores ópticos 100GBase-SR4
- Estándar IEEE 802.3bm
- Módulo tipo QSFP28
- Tasa de transferencia de datos para ethernet 103.1 Gbps
- Rango de transmisión 100 metros, para fibra OM4
- Fibra Multimodo
- Longitud de onda 850 nm
- Conector tipo MPO12
- Potencia disipada < 3.5 W
- Rango de temperatura de funcionamiento 0-70ºC
- Inserción en caliente
- Monitorización digital
- Auto Negociación y Link Status.

6.3 Consola de administración centralizada de los endpoints conectados por VPN SSL

Las características de la consola de administración centralizada de los endpoints son las siguientes:

- Capacidad para gestionar de forma centralizada endpoints Windows, Mac, Linux, Chrome, iOS y Android.
- Gestión del inventario software
  - Visibilidad y gestión de las aplicaciones instaladas y su licenciamiento.
  - Detección y borrado del software innecesario o aplicaciones legacy para reducir la superficie de ataque.
- Integración con Windows AD
  - Sincronización con el Directorio Activo.
  - Uso de las mismas Unidades Organizativas (OUs).
- Estado del endpoint en tiempo real
  - Información de la actividad del endpoint y de los eventos de seguridad.
  - Escaneado de virus y de vulnerabilidades bajo demanda.
- Panel de vulnerabilidades.
  - Gestión de la superficie de ataque de la organización.
  - Identificación de los endpoints vulnerables.
- Despliegue y provisionamiento centralizado del cliente VPN SSL
  - Despliegue del cliente VPN SSL y actualizaciones controladas de forma remota.
  - Capacidad para despliegues masivos.
- Soporte para SandBox on premise (no incluido en este pliego).
- Telemetría

    - Visibilidad en tiempo real del endpoint en las consolas de los Firewalls.
    - Visión unificada de los endpoints en los componentes del Security Fabric.
- Control de acceso dinámico para aplicación del cumplimento normativo.
    - Creación de grupos virtuales basados en el nivel de seguridad del endpoint.
    - Utilización de estos grupos en las políticas de los Firewalls para control de acceso dinámico.
- Cuarentena de los endpoints
    - Desconexión rápida de los endpoints comprometidos.
- Respuesta automática
    - Detección y aislamiento de endpoints comprometidos o sospechosos sin intervención manual.
- Integración
    - Con Security Fabric.
    - Con FortiAnalyzer.

Las características técnicas de los clientes VPN SSL licenciados para la consola de administración centralizada del endpoint son las siguientes:

- Endpoint unificado que incluya cumplimiento, protección y acceso seguro en un único cliente ligero.
- Visibilidad y control end-to-end e integración nativa con Security Fabric
- Protección avanzada contra amenazas, exploits y malware.
    - Protección contra ataques día cero.
    - Detección de técnicas de memoria, como ROP, HeapSpray y buffer overflow.
    - Protección de los navegadores web, plug-ins Java/Flash, aplicaciones Microsoft Office y PDR Reader.
    - Protección basada en la nube.
- Gestión integrada del parcheo de vulnerabilidades de los endpoints.
- Gestión simplificada y cumplimiento de políticas de Firewall.
- Acceso remoto seguro
    - Acceso SSL e IPSec
    - Auto-connect y always-up VPN
    - Segundo factor de autenticación compatible con FortiToken.
    - Selección dinámica del gateway VPN.
    - Capacidad de Split-tunneling.
- Opciones de autenticación:
    - RADIUS, LDAP, Base de datos local, TACACS+, Certificado digital en formato X509, FortiToken o compatible.
- Sistemas Operativos disponibles:
    - Windows
    - Mac OS X
    - Android
    - iOS
    - Chromebook
    - Linux

7. DOCUMENTACIÓN A PRESENTAR

Para llevar a cabo las prestaciones y servicios descritos en este pliego, el adjudicatario deberá presentar los documentos de acreditación expedidos por el fabricante FORTINET y del fabricante del equipamiento de renovación tecnológica y de la consola de administración centralizada del endpoint, en su condición de partner oficial cualificado, capacitándole para la prestación de los servicios de soporte descritos en el Pliego de Prescripciones Técnicas objeto de este contrato.

En concreto para el fabricante Fortinet será la siguiente:

- Certificado emitido por el fabricante como partner ADVANCED o EXPERT.

- Certificación activa NSE 4 para al menos uno de los técnicos de soporte asignados al contrato.

Esta documentación deberá ser presentada en el plazo de un mes a contar desde el día siguiente a la firma del contrato.

8. CONTROL DE CALIDAD

La UAH podrá realizar controles de calidad al objeto de verificar que los suministros y servicios prestados por el adjudicatario se ajustan a las condiciones estipuladas en el presente pliego.

En concreto, verificará la completa compatibilidad, equipamiento suministrado con el ya existente en la UAH, a nivel de funcionalidades de Security Fabric, FSSO, FortiToken e integración con el FortiAnalyzer.

En el supuesto de que alguno de los elementos analizados mostrase deficiencias o incumplimientos de las características técnicas y de calidad requeridas en este pliego, el adjudicatario deberá retirar esos elementos en el plazo de TRES DÍAS a contar desde la comunicación efectuada por escrito por la UAH y reponerlos en las debidas condiciones en el plazo máximo de CINCO DÍAS a contar desde el día siguiente al de la retirada.

9. PREVENCIÓN DE RIESGOS LABORALES

Tanto el adjudicatario como las empresas subcontratadas o trabajadores autónomos contratados por ésta cumplirán en el desarrollo de sus funciones con los requisitos legales que marca la Ley 31/1995 de Prevención de Riesgos Laborales y con el R.D 171/2004, de coordinación de actividades empresariales, en cada caso.

La empresa adjudicataria informará con suficiente antelación al Servicio de Prevención de la UAH (servicio.prevencion@uah.es) cada vez que subcontrate trabajos a realizar en la propia UAH, con otra empresa o trabajador autónomo, indicando la forma de coordinación preventiva establecida entre ellos.

El adjudicatario cumplirá asimismo con el procedimiento de coordinación de actividades empresariales vigente en la UAH en todo aquello que le sea aplicable.

En caso de que un trabajador de la empresa adjudicataria sufra un accidente de trabajo mientras desempeña los servicios contratados por la UAH, la empresa adjudicataria informará asimismo al Servicio de Prevención de la UAH a la mayor brevedad posible.

10. MEDIDAS DE PROTECCIÓN AMBIENTAL

Además de las acciones de reutilización, reciclado o eliminación adecuadas asociadas a la retirada de embalajes, el adjudicatario se compromete a respetar la normativa vigente al respecto, ya sea de carácter estatal, autonómico, local o universitario en la recogida y reciclado de cualesquiera residuos y componentes que pudieran resultar de las actuaciones del servicio prestado a la UAH.