Escuela Andaluza de Salud Pública
Consejería de Salud y Consumo

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR LA CONTRATACION DEL SUMINISTRO, INSTALACIÓN, MIGRACIÓN Y PUESTA EN MARCHA DE ELECTRONICA DE RED Y FIREWALL FÍSICOS (APPLIANCES) PARA LA SEGURIDAD PERIMETRAL DE LA ESCUELA ANDALUZA DE SALUD PUBLICA.

11 DE DICIEMBRE DE 2024

ESCUELA ANDALUZA DE SALUD PUBLICA
Carretera del Observatorio 4, Campus Universitario de Cartuja, CP 18011 Granada

INDICE.

INDICE DE TABLAS Y FIGURAS

1. ANTECEDENTES

La Escuela Andaluza de Salud Pública, ubicada en Carretera del Observatorio 4, Campus Universitario de Cartuja, CP 18011 Granada, tiene desplegada una red de área local (LAN), para interconectar los dispositivos electrónico e informáticos. Cuenta también con una solución de seguridad basada en dos cortafuegos en la citada sede. Esta red LAN y solucion de seguridad, fueron puesta en funcionamiento en 2011, por lo que necesitan actualización y mantenimiento de sus componentes electrónicos, ya que es crítica y necesaria para el normal funcionamiento y la gestión de la Escuela.

Los dispositivos electrónicos que conforman esta red son antiguos en su mayoría y no cumplen con las especificaciones necesarias en seguridad de la información por lo que es necesario su renovación tanto de la red LAN como de la solucion de seguridad.

Ante el contexto creciente en complejidad y número de ciberataques a los que nos encontramos expuestas todas las administraciones, agravado si cabe por la pandemia, se hace imprescindible que desde las Administraciones Públicas podamos contar con los recursos, tanto tecnológicos como humanos, que nos permitan gestionar de forma adecuada la seguridad de nuestras infraestructuras, comunicaciones y servicios digitales prestados, mejorando nuestras capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

El proceso de digitalización abre enormes oportunidades al desarrollo socioeconómico, pero al mismo tiempo incorpora amenazas y riesgos relacionados con la seguridad digital en una doble vertiente: el daño causado por los incidentes cibernéticos en sí mismos, y el socavamiento de la confianza en el uso de las tecnologías digitales, que puede afectar a su adopción por parte de los actores económicos y la ciudadanía. Estos dos factores, protección frente a las amenazas y generación de confianza, tienen un impacto directo en el desarrollo económico del país y confirman que la ciberseguridad debe ser abordada desde una perspectiva multidimensional, como elemento clave de la seguridad nacional. Para mitigar este riesgo, es imprescindible el desarrollo de las capacidades de ciberseguridad de ciudadanía, empresas y Administraciones Públicas, así como la generación de confianza a través de una cultura de ciberseguridad que llegue a todas las capas de la sociedad.

Con el objetivo de desarrollar las capacidades necesarias de seguridad en La Escuela Andaluza de Salud Pública, para garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados y mejorar las capacidades de prevención, detección y respuesta ante incidentes, La Escuela Andaluza de Salud Pública, plantea la contratación de diversas actuaciones, como son la renovación de la electrónica de red y la adecuación se los sistemas de Seguridad.

2. 0BJETO.

El presente pliego técnico tiene por objeto la definición de los requisitos técnicos que han de regir la contratación del suministro con instalación y puesta en funcionamiento de dispositivos de red inteligentes (Smart Switches) y de la solución integral de seguridad de Nueva Generación (en adelante, NGFW) configurados en alta disponibilidad, para la Escuela Andaluza de Salud Pública.
La Escuela Andaluza de Salud Pública ha evaluado las características necesarias que han de cumplir los dispositivos que se entienden necesarios para mejorar la infraestructura de la red LAN y seguridad. Estas características son de obligado cumplimiento.

Para dar respuesta a los principios de actuación referentes a la seguridad y protección de datos personales descritos en las leyes 39 y 40 del 2015 y con el objetivo de garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados y mejorar las capacidades de prevención, detección y respuesta ante incidentes, la Escuela Andaluza de Salud Pública plantea la contratación de una serie de soluciones, todas ellas relacionadas con la seguridad de la información y orientadas a conseguir los siguientes objetivos:

1. Renovación de la electrónica de red (suministro del equipamiento de red) y de la actual Plataforma ciberseguridad para actualizar las infraestructuras actuales.
2. Formar a la plantilla técnica del departamento de informática y nuevas tecnologías sobre cómo administrar y gestionar las posibles incidencias de CiberSeguridad con la nueva infraestructura a desplegar.
3. Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por la Escuela Andaluza de Salud Pública y mejorar las capacidades de monitorización de la seguridad, prevención, detección temprana, la vigilancia y análisis de diversas fuentes de amenaza y vulnerabilidades y, finalmente, optimizando la capacidad de reacción, respuesta y recuperación ante cualquier posible incidente. Para la consecución de este objetivo, se proponen dos líneas de actuación para solventar las carencias detectadas en nuestras instalaciones, que son:
   a) Por un lado, el suministro, la implantación y configuración de la infraestructura de red necesaria que permita la aplicación de las políticas de seguridad y de control de acceso a la red interna (NAC). Nuestra actual electrónica de red, al ser ya obsoleta, no permite la integración con nuestro NAC, por lo que no pueden aplicarse correctamente estas políticas de seguridad a nivel de control de acceso al medio en los switches. Se pretende por tanto actualizar nuestra actual electrónica de red, para que en el futuro podamos implantar políticas de control de acceso al medio.
   b) La prestación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en las transacciones de los sistemas de información y comunicaciones de la Escuela Andaluza de Salud Pública, así como optimizar la capacidad de reacción, respuesta y recuperación ante cualquier posible incidente.

Para conseguir estos objetivos, se propone la contratación de una serie de soluciones atendiendo a las características de los trabajos a realizar:

- Renovación de la electrónica de red (suministro del equipamiento de red) y Formación avanzada para el personal técnico en la gestion y administración de la nueva plataforma.
- Renovación de la plataforma ciberseguridad y Formación avanzada para el personal técnico en la gestion y administración de la nueva plataforma.

El presente contrato debe considerarse como CONTRATO MIXTO, siendo la prestación principal la de suministro.

3. CONDICIONES GENERALES

Con carácter general, la empresa adjudicataria deberá prestar un servicio integral que abarque todos los aspectos relacionados como el suministro, reciclaje, instalación, configuración, puesta en marcha y garantía de los diferentes sistemas suministrados.
Por otra parte, el adjudicatario será el responsable del correcto licenciamiento tanto del hardware como del software incluido en el suministro de acuerdo con las especificaciones de los fabricantes de las soluciones que formen parte de su oferta (Soporte de fabricante), haciéndose cargo del coste de estas. La Escuela Andaluza de Salud Pública no se hará responsable de las posibles obligaciones que se devengan de un licenciamiento incorrecto en cualquiera de los productos o soluciones ofertadas.

3.1. CARACTERÍSTICAS TÉCNICAS

Para el suministro de equipamiento hardware como parte del alcance del mismo, éste deberá cumplir con los siguientes requisitos:

- Únicamente se admitirán marcas de equipos con reconocimiento internacional, con representación oficial en el territorio español y con canales de distribución de ámbito nacional.
- Serán equipos nuevos, de fabricación reciente y el modelo ofertado estará aún vigente en el catálogo de productos del fabricante. No se admitirá equipamiento ni accesorios reacondicionados.
- Todos los equipos y accesorios suministrados estarán en garantía durante el tiempo indicado en el documento o, en caso de que exista mejora, en el tiempo ofertado.

Se informa a los licitadores, que las características técnicas de los equipos que se indican en los siguientes apartados, se han obtenido de descripciones y catálogos de diversas marcas comerciales, tratándose en la mayoría de los casos de requisitos técnicos mínimos y se aceptarán características equivalentes o superiores con independencia de las marcas fabricantes de los equipos que han servido de base para la descripción de estos.
En todos los casos el equipamiento a suministrar sustituirá a un equipamiento existente, en cuyo caso, se incluirá en el pliego una descripción de las características técnicas básicas que debe cumplir el equipamiento nuevo a suministrar. Estas referencias deberán interpretarse como una orientación, dejando libertad al licitador para ofertar un modelo equivalente siempre y cuando las características técnicas sean iguales o superiores a las indicadas.

En el caso de que la documentación técnica aportada por el licitador incluya en la descripción de los productos ofertados más de un valor para una misma característica técnica, por ejemplo: *rendimiento del switch (switch throughput): 10/20 Gbps*. Se entenderá como válida la cifra más desfavorable, salvo que se especifique claramente el motivo de aportar dos valores y cuál es la interpretación de cada uno de ellos.

3.2. PROPIEDAD INTELECTUAL

Toda la documentación que se genere como parte de los trabajos incluidos, se entregará en formato electrónico y será propiedad de la Escuela Andaluza de Salud Pública, quien se reserva el derecho de reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el autor material de los trabajos.

El adjudicatario renunciará de forma expresa a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiese corresponderles, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en este contrato, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin la autorización expresa de la Escuela Andaluza de Salud Pública.
Respecto al licenciamiento de los productos software incluidos, el adjudicatario deberá facilitar la documentación necesaria donde se acredite el licenciamiento de todos los productos incluidos.

3.3. CONFIDENCIALIDAD

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del servicio contratado, tanto aquella suministrada directamente por la Escuela Andaluza de Salud Pública a través de cualquier medio, así como toda aquella información que pudiera ser extraída, producida, o derivada, fruto de la realización del propio servicio.
Esta información será utilizada por el adjudicatario exclusivamente para los fines propios del servicio objeto del presente contrato. Dicha información, no podrá ser entregada o transferida a terceras partes, sean estas personas físicas o jurídicas en ninguna circunstancia y continuará en toda su extensión y efectos por un período ilimitado.
El adjudicatario estará obligado a poner en conocimiento de la Escuela Andaluza de Salud Pública, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

3.4. EXIGENCIAS MEDIOAMBIENTALES

El adjudicatario será el responsable de retirar y reciclar adecuadamente todos los equipos, repuestos y piezas de aquellos equipos que sean retirados.
También será responsabilidad del adjudicatario la separación y reciclado de todos los embalajes empleados en el suministro y sustitución de equipos y piezas.

3.5. DURACIÓN DEL CONTRATO

La duración del contrato será de 3 AÑOS.

4. SITUACIÓN ACTUAL

Actualmente La Escuela Andaluza de Salud Pública, cuenta con el siguiente equipamiento:

4.1. ELECTRONICA DE RED

El edificio cuenta con tres armarios de comunicaciones (CPD, secretaria y Aulas) con una distribución de tomas articuladas en torno a estos 3 armarios de reparto, siendo uno de ellos el CPD. Entre ellos existen tiradas de fibra óptica de 8 núcleos OM3, con lo que se constituye un diseño en triangulo cerrado para redundancias.

4.1.1. INTERCONEXIÓN FÍSICA DE ARMARIOS

La solución implantada en la planta alta o pila de secretaría es la siguiente.

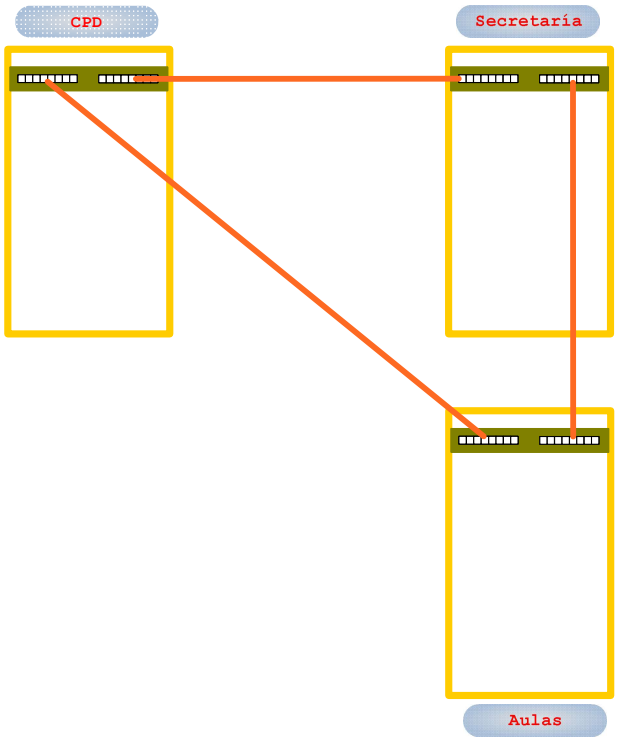

Figura 1: Interconexión física de los Armarios

Sobre este diseño de fibra se establece la actual interconexión de la electrónica instalada con las siguientes conexiones.

- Un enlace de 10Gb entre cada pila y el equipo de CORE (enlace principal)
- Un enlace de 1 Gb como servicio de respaldo entre cada nodo de la red.

Estas interconexiones están implantadas atendiendo a un criterio de redundancia (la caída de una supervisora no deja sin servicio a una planta) y de simplicidad de configuración en los armarios de las pilas (configuraciones iguales en las dos pilas).

4.1.2. ARMARIO DE AULAS

La solución implantada en la planta baja o pila de aulas es la siguiente.

Pila Aulas		
Modelo	Descripción	Equipos
Equipamiento		
WS-C2960S-48LPD-L	Catalyst 2960S 48 10/100/1000T + 2 x 10 GB SFP + IPB Image 370W· Poe	2
WS-C2960S-48TS	Catalyst 2960S 48 10/100/1000T + 4 SFP + IPB Image	2
C2960S-STACK	Module Stack + cable 2960S	4
Ópticas		
SFP-10G-LMR	Catalyst SFP 10GBase LRM (Largo alcance. 220m en fibra 62.5)	1
1000BaseSX SFP	1000BaseSX SFP	2

Tabla 1: Pila de Aulas

Estos equipos están configurados en una única pila, en la cual uno de ellos actúa como MÁSTER de la pila.

4.1.3. ARMARIO DE SECRETARIA

La solución implantada en la planta alta o pila de secretaría es la siguiente.

Pila secretaria		
Modelo	Descripción	Equipos
Equipamiento		
WS-C2960S-48LPD-L	Catalyst 2960S 48 10/100/1000T + 2 x 10 GB SFP + IPB Image 370W· Poe	2
WS-C2960S-48TS	Catalyst 2960S 48 10/100/1000T + 4 SFP + IPB Image	2
C2960S-STACK	Module Stack + cable 2960S	4
Ópticas		

SFP-10G-LMR	Catalyst SFP 10GBase LRM (Largo alcance. 220m en fibra 62.5)	1
1000BaseSX SFP	1000BaseSX SFP	2

Tabla 2: Pila de secretaria

Estos equipos están configurados en una única pila, en la cual uno de ellos actúa como MÁSTER de la pila.

4.1.4. CPD

La solución implantada en el CPD es la siguiente.
El CORE de la red este compuesto por un equipo C4510R+E, en el cual dispone de dos tarjetas supervisoras de alta capacidad y un conjunto de tarjetas de distintas prestaciones y anchos de banda, para dar servicio tanto a los servidores instalados en el CPD como a una gran cantidad de usuarios situados en la planta alta.
Además, dispone de dos fuentes de alimentación de 2800W, por redundancia al sistema mediante la incorporación.

SLOT		Product Id
Chasis		WS-C4510RE-S7+96V+
PS1		PWR-C45-2800ACV
PS2		PWR-C45-2800ACV
FAN		WS-X4582+E
1		WS-X4648-RJ45-E=
2		WS-X4648-RJ45-E=
4		WS-X4648-RJ45V+E=
5		WS-X45-SUP7-E
	5.1	SFP-10Gbase-LRM
	5.2	1000BaseSX
6		WS-X45-SUP7-E
	6.1	SFP-10Gbase-LRM
	6.2	1000BaseSX
9		WS-X4748-RJ45V+E
10		WS-X4748-RJ45V+E

Tabla 3: CORE CPD

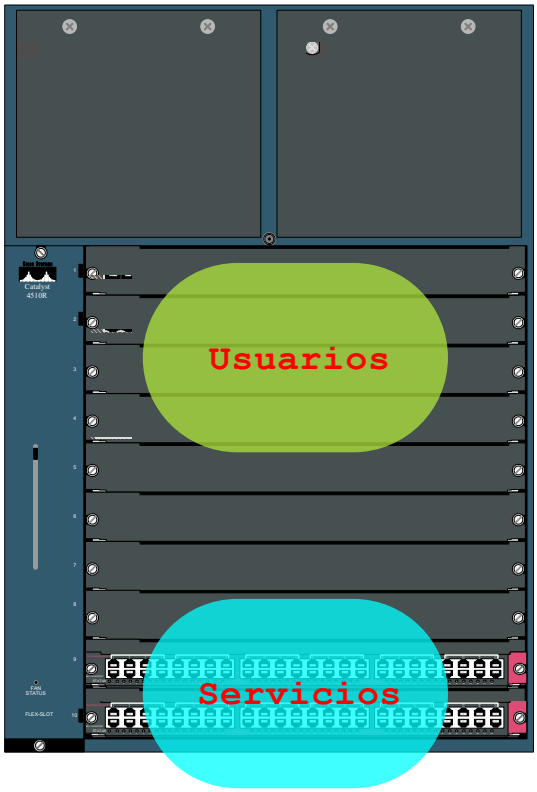

Figura 2: CPD CORE

El CORE cuenta con dos zonas diferenciadas. La primera de ellas está ubicada en la parte superior del chasis (de las supervisoras hacia arriba) y está destinada a dar servicio a los usuarios. Está compuesta por tarjetas POE y no POE, por lo que atiende estas necesidades. El segundo bloque está formado por dos tarjetas de altas prestaciones y está destinado a conectar con los servidores, los puntos de acceso y otros dispositivos especiales, y los firewalls.

4.1.5. INTERCONEXIÓN DE LAS PILAS

La interconexión interna de los 4 elementos que conforman las pilas esta realizado mediante un módulo de stack. Los enlaces se han realizado mediante una distribución en tresbolillo que permite separar los dispositivos unos centímetros más que la típica de anillo.

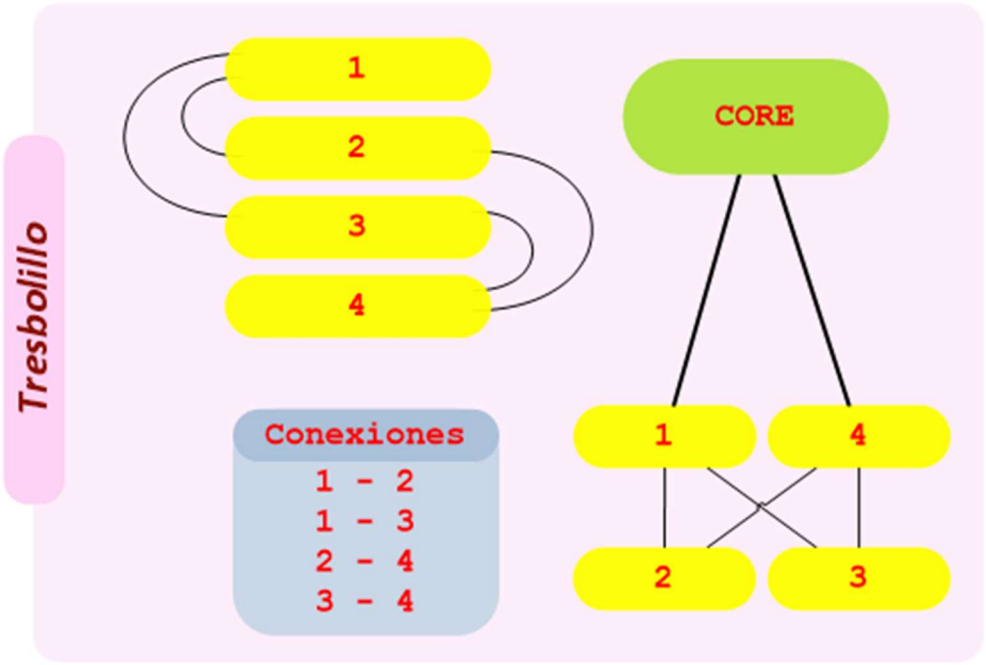

Figura 3: DISTRIBUCIÓN EN TRESBOLILLO

4.1.6. CAPACIDAD PoE ACTUAL

En la actualidad hay una gran cantidad de puertos con capacidades de PoE. La distribución por armarios es la siguiente:

Equipo	Ubicación	Puertas
C4510	SLOT 4	48
C4510	SLOT 9	48
C4510	SLOT 10	48
Secretaría	Switch 1	48
Secretaría	Switch 4	48
Aulas	Switch 1	48
Aulas	Switch 4	48
	Total	**336**

Tabla 4: PUERTOS POE

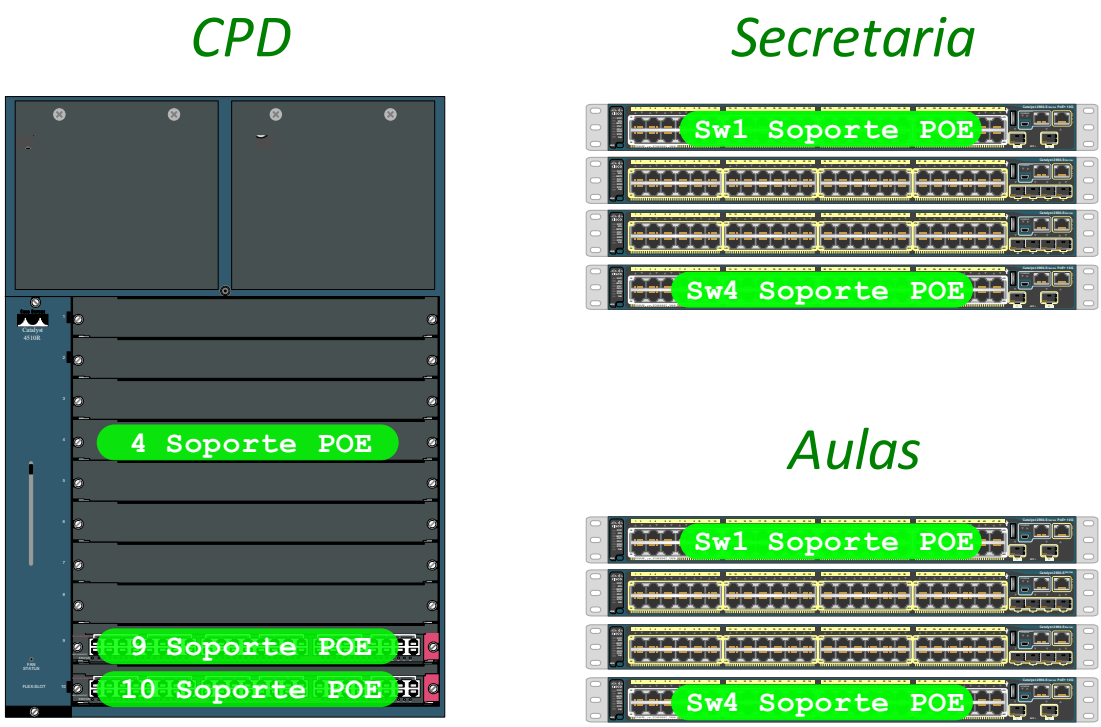

Figura 4: PUERTOS POE ACTUALES

4.1.7. DHCP

El direccionamiento IP de los usuarios es gestionado por DHCP.
El C4510 y los firewalls actúan como Relay de las peticiones DHCP.

4.2. FIREWALLS

Actualmente la Escuela Andaluza de Salud Pública, cuenta con 2 firewalls perimetrales para la seguridad de todos los equipos informáticos de la propia entidad, dicho equipamiento actual ya no satisface las necesidades actuales de esta entidad (velocidad, rendimiento, fiabilidad, consumo, etc), además de que es equipamiento antiguo y en un futuro cercano el fabricante ya no podrá mantenerlo, por lo tanto, se requiere nuevo equipamiento en el ámbito de la seguridad informática perimetral con su mantenimiento activo por parte del fabricante que cubra las necesidades actuales y futuras de la Escuela Andaluza de Salud Pública.

Firewall		
Equipo	Puertas	Descripción
Routers	Gi9/27	Router RCJA
	Gi10/28	Router RCJA
	Gi9/25	Router

Firewall		
Equipo	Puertas	Descripción
Firewall Albaicin	Gi9/14	Srv-EXT FW
	Gi9/26	ONO FW albaicin po
	Gi9/28	RCJA FW
	Gi9/35	WIFI FW 30,97
	Gi9/36	WIFI Invitados-FW
	Gi9/38	LanEASP FW
	Gi9/45	FW Srv-BD Srv-DES
	Gi10/45	FW Srv-BD Srv-DES
Firewall Sacromonte	Gi10/13	Srv-EXT FW
	Gi10/25	ONO FW sacromonte
	Gi10/27	RCJA FW
	Gi10/35	WIFI Invitados-FW
	Gi10/36	WIFI FW 30,97
	Gi10/37	LanEASP FW
	Gi9/46	FW Srv-BD Srv-DES
	Gi10/46	FW Srv-BD Srv-DES

Tabla 5: PUERTOS USADOS

5. RENOVACIÓN ELECTRÓNICA DE RED

La Escuela Andaluza de Salud Pública cuenta en estos momentos con una infraestructura de red ya incapaz de proporcionar, en las debidas condiciones, respuesta al indudable crecimiento de los servicios ofrecidos a través de la red.
La electrónica de red, tal como se aporta en el apartado situación actual, tienen una antigüedad que supera los 13 años, siendo habitual que la mayoría de estos dispositivos ya no dispongan de soporte.
Debido a la antigüedad, nos encontramos con barreras infranqueables a la hora de poder llevar a cabo nuevos proyectos TIC.

por tanto, para la contratación del suministro de la infraestructura de electrónica de red, del edificio, se desea actualizar la electrónica de red, por otra que se adapte a las nuevas necesidades, permitiéndonos un crecimiento futuro tanto a nivel de número de conexiones, velocidad de transferencia y de nuevas funcionalidades tales como aplicación de políticas de seguridad por medio de ACL's, VoIP, PoE, etc.
CPV: 32422000-7 – Componentes de Red.

5.1. ALCANCE

La contratación incluirá tanto el suministro, como los servicios necesarios de actualización del software y transporte del equipamiento suministrado, de forma que todo el equipamiento adquirido quede plenamente operativo en los términos que se describen en los siguientes apartados.
En este apartado se describen las características técnicas y condiciones mínimas que deberán cumplir los bienes y servicios objeto de la presente contratación.
Conforme se establece en los siguientes apartados, el adjudicatario deberá actualizar el firmware, transportar y entregar todo el equipamiento suministrado.

En la siguiente tabla, se muestran el alcance de este proyecto y se indican las necesidades de equipamiento a suministrar.

Ubicación Equipo	Switches	Puertas	Con POE
CORE	5x48	240	48
Secretaría	4x48	192	48
Aulas	4x48	192	48
Total		**624**	**144**

Tabla 6: PUERTOS REQUERIDOS

En cada armario los equipos estarán apilados por lo que contarán con capacidad para conectar y gestionar múltiples switches como una única unidad lógica mediante apilamiento físico.
Se deberá suministrar y aporta todo lo necesario para que la solucion quede totalmente operativa y en funcionamiento.
Todos los enlaces entre armarios se realizarán a 10 Gbps mediante la actuales F.O.

5.1. CARACTERÍSTICAS TÉCNICAS DEL EQUIPAMIENTO DE RED A SUMINISTRAR

Generales

- Los switches deben ser compatibles e integrables a la solución de definición de red Cisco SD-Access.
- Los equipos ofertados deben soportar Cisco Trustsec.
- Los equipos ofertados deben ser capaces de soportar imágenes Cisco IOS.
- Los equipos deben ser capaces de soportar fuentes redundantes y distintos tipos de fuentes en el mismo chasis: AC/AC, AC/DC y DC/DC.
- Los switches deben ser compatibles con el esquema de suscripciones Cisco DNA y poder ser capaces de modificar upgrade/downgrade el nivel de suscripción durante la vigencia de esta.

Diseño Integral para Operación Confiable

Tanto el CORE como los switches de acceso deben operar en un rango de temperatura de 0°C a 45°C, con tolerancia a niveles de humedad relativa de hasta el 85% sin condensación. Su diseño debe incluir compatibilidad con racks estándar de 19 pulgadas y ofrecer accesorios para una instalación segura.

Estas características aseguran que la infraestructura de red cumpla con las demandas de conectividad, seguridad y escalabilidad, alineándose con los estándares actuales de tecnología empresarial.

5.1.1. EQUIPAMIENTO CORE:

Robustez Y Alta Disponibilidad

El núcleo de la red (CORE) debe garantizar un alto rendimiento, confiabilidad y escalabilidad para soportar las demandas de tráfico actuales y futuras. Por ello, se exigen las siguientes características:

Puertos y Conectividad

El equipo CORE debe ofrecer un mínimo de **4 puertos de uplink** con velocidades de 10 Gbps, compatibles con módulos SFP+. Además, debe permitir opciones de crecimiento hacia **25 Gbps** en escenarios futuros. Esto asegura conectividad de alta velocidad tanto para enlaces internos como externos.

Rendimiento Excepcional

El CORE debe manejar un tráfico intenso con una capacidad de conmutación mínima de **176 Gbps** y un rendimiento de reenvío de al menos **130 Mpps**. La memoria buffer dedicada, con un mínimo de **3 MB por puerto**, permite gestionar picos de tráfico sin pérdidas de paquetes. Esto lo hace adecuado para redes empresariales de gran escala.

Escalabilidad y Apilamiento

Debe ser posible gestionar hasta **8 dispositivos apilados** como una sola unidad lógica, con un ancho de banda interno entre ellos de **160 Gbps**. Además, la redundancia automática en el apilamiento garantiza la continuidad de la operación ante fallos en cualquier miembro de la pila.

Gestión Centralizada y Seguridad Avanzada
El CORE debe ser compatible con herramientas de gestión basadas en **SNMP**, soportar protocolos de descubrimiento como **LLDP**, y ofrecer interfaces tanto gráficas como de línea de comandos para su administración. En términos de seguridad, debe incluir **autenticación 802.1X**, soporte para **MACsec** para cifrado de tráfico, y mecanismos como **DHCP Snooping** e **IP Source Guard** para proteger contra ataques malintencionados.

Eficiencia y Diseño Modular
El cumplimiento con estándares de eficiencia energética como **IEEE 802.3az** y la certificación **80+ Platinum** garantizan un consumo optimizado. Además, su diseño modular con ventilación intercambiable asegura un funcionamiento confiable en entornos de alta densidad.

5.1.2. EQUIPAMIENTO DE ACCESO:

Los switches de acceso son esenciales para la conectividad de los dispositivos finales en la red. Las siguientes características aseguran su desempeño óptimo:

Puertos Versátiles
Cada switch debe contar con al menos **48 puertos RJ45** compatibles con velocidades de **10/100/1000 Mbps**, permitiendo conexiones confiables para estaciones de trabajo, teléfonos IP y puntos de acceso inalámbrico. Adicionalmente, debe incluir **4 puertos uplink SFP+** a 10 Gbps con capacidad para agregación de enlaces mediante **LACP**.

Capacidad para Redes Virtuales
El soporte para **4000 VLANs** activas garantiza una segmentación eficiente del tráfico y una gestión ordenada de la red. Los puertos deben permitir asignación dinámica a VLANs mediante **802.1Q** y ofrecer priorización de tráfico mediante **QoS (802.1p).**

Apilamiento y Resiliencia
La capacidad de apilar hasta **8 switches** y administrarlos como un solo dispositivo permite una mayor simplicidad en la gestión. El apilamiento debe incluir redundancia automática para mantener la operación en caso de fallos.

Protección y Seguridad
Los switches de acceso deben implementar características de seguridad avanzadas, como:
- **Autenticación mediante 802.1X** con integración a servidores RADIUS o TACACS+.
- **Listas de control de acceso (ACLs)** basadas en IP, MAC y protocolos, aplicables a nivel de puerto.
- Mecanismos de protección como **DHCP Snooping, Port Security**, y mitigación de ataques **DoS**.

Gestión y Automatización
Los switches deben ser compatibles con sistemas de monitoreo y gestión basados en **SNMP** y permitir configuraciones mediante interfaces gráficas (GUI) o de línea de comandos (CLI). Además, deben soportar despliegues automatizados mediante herramientas **Plug-and-Play**.

Rendimiento y Eficiencia

Con una capacidad mínima de conmutación de **176 Gbps** y soporte para al menos **32K direcciones MAC**, estos equipos están diseñados para soportar entornos de alta densidad. La eficiencia energética, asegurada mediante **IEEE 802.3az**, reduce costos operativos y respalda el compromiso ambiental.

6. RENOVACIÓN CORTAFUEGOS

La Escuela Andaluza de Salud Pública cuenta en estos momentos con una infraestructura de seguridad incapaz de proporcionar, en las debidas condiciones, respuesta al indudable crecimiento de los servicios actuales y futuros.

En este apartado se definen los requerimientos básicos de los sistemas de seguridad, así como los servicios adicionales en los términos descritos en los siguientes apartados.
...
El servicio que se demanda consiste en el suministro de una solución integral constituida por los siguientes elementos:

- Firewalls de Nueva Generación (en adelante, NGFW) configurados en alta disponibilidad, con funcionalidades de:
  - Firewall Stateful Inspection
  - Detección y prevención de intrusiones.
  - Inspección de tráfico cifrado SSL.
  - Identificación de aplicaciones, usuarios y dispositivos.
  - Antivirus.
  - Control de accesos a páginas web, clasificadas por categorías.
- Sistema de seguridad Antivirus/Antibotnet y Antispam
- Actualización durante 3 años de todas las licencias usadas.

Con el fin de dar cumplimiento al Esquema Nacional de Seguridad deberán proponerse equipos cuyo fabricante esté validado en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación del Centro Criptológico Nacional, Guía de Seguridad de las TIC CCN-STIC 105. Los equipos cortafuegos propuestos han de disponer de GUIA CCN CERT para servir de guía durante el periodo de servicio para la instalación, operación y mantenimiento de los cortafuegos.

Los licitadores presentarán una única oferta sin alternativas ni variantes.

En el siguiente apartado se especifican los requisitos mínimos obligatorios que deben cumplir los equipos ofertados.

La contratación incluirá tanto el suministro, como los servicios necesarios de actualización del software y transporte del equipamiento suministrado, de forma que todo el equipamiento adquirido quede plenamente operativo en los términos que se describen en los siguientes apartados.
En este apartado se describirán las características técnicas y condiciones mínimas que deberán cumplir los bienes y servicios objeto de la presente contratación.
Conforme se establece en los siguientes apartados, el adjudicatario deberá actualizar el firmware, transportar y entregar todo el equipamiento suministrado.

Sistema NGFW

Se requiere el suministro e instalación de un cluster constituido por 2 equipos NGFW en alta disponibilidad, permitiendo tanto modo activo-activo como activo-pasivo, con las siguientes características técnicas mínimas:

- Rendimiento mínimo del servicio Firewall IPV4/IPV6: 26 Gbps.
- Rendimiento mínimo del servicio VPN (IPSec): 12 Gbps.
- Rendimiento mínimo NGFW (IPS+control de aplicaciones, tráfico Enterprise Mix): 1.7 Gbps.
- Rendimiento mínimo Threat Prevention (IPS+control de aplicaciones+Antimalware, tráfico Enterprise Mix): 2.7 Gbps.
- Capacidad mínima de gestión de conexiones. 2.500.000 sesiones concurrentes, permitiendo como mínimo 250.000 nuevas sesiones por segundo.
- Número mínimo de interfaces 10 GE SFP+: 4. (incluir transceivers)
- Número mínimo de interfaces GE: 16.
- Número mínimo de puertos con interface SFP: 8.
- Posibilidad de disponer de un puerto específico de gestión o puerto disponible en el dispositivo para su uso con tecnologías Ethernet dedicado con el objetivo de garantizar que no consuma interfaces de servicio para esta tarea.
- Disco interno: 1x480GB de tipo SSD
- Dominios virtuales mínimos: 10.
- Latencia máxima: 4.78 µs.

Los rendimientos indicados han de ser medidos en condiciones reales/traffic mix, no aceptándose valores medidos en condiciones ideales. Debe indicarse explícitamente en la propuesta cuáles son las condiciones de medida de los valores suministrados.

Las características funcionales de los servicios que deberán integrar los sistemas NGFW requeridos, son las siguientes:

- Firewall:
    - Inspección profunda de contenido.
    - Múltiples modos de despliegue (modos mirror, transparente y NAT/PAT).
    - Capacidades de Routing estático, policy based routing y routing dinámico, soportando BGP, OSPF, Rip v2 y Multicast, tanto para IPv4 y IPv6.
    - Gestión de VLAN e integración de 802.1Q.
    - Autenticación basada en grupos de usuarios.
    - Capacidad de securización de VoIP.
    - Protección basada en la creación de perfiles aplicables a usuarios individuales y/o grupos.

- NETWORKING
    - Es necesario que la solución de seguridad tenga capacidades de SD-WAN, en concreto:
        - Balanceo inteligente de conexiones físicas y lógicas, indiferentemente del tipo de conexión WAN (MPLS, 3G / 4G, FTTH, VPN, etc.).
        - El número mínimo de conexiones físicas y lógicas que se pueden añadir a la SD-WAN debe ser de al menos 4 líneas para balancear.
        - Chequeo de parámetros avanzados: jitter, packet loss y latencia por línea.

  - Configuración de políticas de SD-WAN inteligentes basadas en origen (usuarios AD y dirección IP), en el destino (dirección IP, aplicaciones y/o servicios de Internet) y en la línea con mejor calidad de aquel momento (basado en valores de jitter, packet loss, latencia, tráfico de subida/bajada o ancho de banda, así como una combinación de las mismas mediante pesos).
  - Estas funcionalidades deben estar disponibles en los equipos cortafuegos sin necesidad de ninguna licencia adicional

- Es necesario que el puerto USB se pueda conectar un módem 3G/4G para usarlo como conexión a Internet o backup.
- Capacidades de VXLAN y VXLAN VTEP para la extensión de redes de nivel 2 entre redes de nivel 3.
- El sistema propuesto debe tener una funcionalidad integrada de Traffic Shaping, siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este traffic shaping debe basarse en aplicaciones y URLs.
- Soporte de protocolos RIP v1 / v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6.
- Routing basado en política o PBR.
- Soporte Dual Stack IPv4 e IPv6 simultáneamente.
- Network address translation NAT IPv4, NAT64 y NAT66.
- DHCP server / DHCP Relay / DNS Server / 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 por la agregación de puertos.
- Las interfaces que conforman los enlaces SD-WAN deben poder ser monitorizados de forma constante permitiendo guardar en los sistemas correspondientes un histórico de su estado en términos de cumplimiento de los diferentes SLAs definidos.
- La solución planteada debe permitir identificar un mínimo de 4.000 aplicaciones. Esta identificación podrá emplearse como parte de las políticas de WAN Steering, la monitorización de health-checks de los servicios y la aplicación de políticas de QoS.

- VPN (Virtual Private Network):
  - Protocolos soportados: PPTP, IPSec y SSL.
  - Cifrado y autenticación: DES, 3DES y AES. SHA1 y MD5.
  - Modo de funcionamiento cliente/servidor y punto a punto.
  - Cliente VPN propietario que asegure la integración con los sistemas ofertados.
  - Modo proxy inverso que permita la publicación mediante portal web de aplicaciones tipo WEB, RDP, SSH, Acceso a carpetas y VNC.
  - Cliente VPN gratuito para sistemas operativos IOS y Android.
  - Funcionalidad integrada del mismo fabricante de doble factor de autenticación vía token móvil, así como por SMS y correo electrónico, integrado en la misma plataforma de seguridad. Este token también se debe poder utilizar para el acceso seguro de administración a la GUI de los equipos cortafuegos.

- Inspección de tráfico cifrado
  - Soporte para TLS 1.3.
  - La solución propuesta ha de ser capaz de inspeccionar tráfico SSL y SSH, sin que el descenso de rendimiento sea superior al 30%.

- Protección Antimalware:
  - Protocolos que se requieren analizar: HTTP/HTTPS, POP3/POP3S, FTP, SMTP/SMTPS, IMAP/IMAPS, MAPI, mensajería instantánea.
  - Posibilidad de bloqueo de ficheros por tipo y tamaño.
  - Posibilidad de gestión de archivos en cuarentena.
  - Servicio de actualización de firmas de virus al menos 3 veces al día.
  - Servicio Antibotnet.
  - Posibilidad de eliminar contenido dinámico de los ficheros analizados.
  - Posibilidad de controlar infecciones de virus entre actualizaciones de las firmas del fabricante.
  - Posibilidad de envío de cierto tipo de ficheros (parametrizable por el administrador) a una plataforma de sandboxing para la detección de ataques de dia cero y amenazas persistentes avanzadas (APTs).

- Servicio IPS (Intrusion Prevention System):
  - Análisis de tráfico e inspección IPS basado en los estándares de los diferentes protocolos.
  - Debe disponer de más de 10.000 firmas de IPS.
  - Deben poder configurarse por parte de los administradores en función de los elementos a proteger (cliente, servidor, tecnología, etc.) .
  - Deben actualizar las firmas al menos 2 veces por semana.
  - Posibilidad de creación y edición de firmas personalizadas.

- Servicio de Filtrado Web:
  - Protocolos a analizar: HTTP/HTTPS.
  - Categorización de contenidos web basado en diferentes categorías
  - Creación de patrones para la definición de listas URL.
  - Bloqueo de contenidos web.
  - Posibilidad de fijación de cuotas de navegación (tiempo y volumen de tráfico) por categoría.
  - Servicio de actualización en tiempo real de categorización de URL.
  - Posibilidad de solicitar la recategorización de páginas web

- Servicio de Control de Aplicaciones.
  - Control de más de 3.000 aplicaciones con independencia de los puertos y protocolo utilizados.
  - Identificación y control de aplicaciones categorizadas por tipo y funcionalidad.
  - Posibilidad de aplicar QoS por aplicación o grupo de aplicaciones, así como a nivel de usuario o grupo de usuarios, permitiendo tanto limitar el ancho de banda como fijar un ancho de banda garantizado.

- Posibilidad de solicitar la identificación de nuevas aplicaciones.
- Disponibilidad de un servicio de actualizaciones de nuevas aplicaciones.

- ZTNA (Zero Trust Network Access):
  - La solución debe permitir definir accesos remotos seguros a los recursos corporativos aplicando el modelo de Zero Trust, como evolución del sistema tradicional basado en VPNs. Para ello el sistema deberá permitir habilitar el acceso a los recursos evaluando diferentes elementos antes de otorgar el acceso a los mismos:
    - Identidad del dispositivo: identificación del dispositivo a través de certificado facilitado por la propia plataforma de gestión
    - Identidad del usuario: con posibilidad de integración LDAP, SAML (SSO) o RADIUS y capacidades MFA (utilizando segundo factor de autenticación mediante OTP [One Time Password] de un modo similar al descrito en el apartado de VPN).
    - *Security Posture* del dispositivo: análisis del estado del dispositivo para su clasificación en términos de seguridad como mínimo en base a conceptos como:
      - Vulnerabilidades detectadas
      - Pertenencia a dominio
      - Existencia de antivirus
      - Versión de SO
  - La funcionalidad ZTNA proporcionada debe permitir realizar la inspección continua del estado de seguridad del endpoint durante todo el tiempo de vida de la conexión, y no sólo durante la fase de establecimiento inicial de la misma, mediante un control continuo de dichos parámetros para -en base a las políticas definidas- poder interrumpir en cualquier momento y de manera automatizada el acceso a los recursos ZTNA definidos.
  - El acceso a las aplicaciones y servicios podrá configurarse de forma granular en base su tipología, incluso accediendo de forma transparente al direccionamiento interno de dichos recursos, para poder habilitar los accesos correspondientes a través de HTTP/HTTPS o mediante redirección de puertos TCP, pero siempre bajo un contexto ZTNA, y no en la forma tradicional de publicación de aplicaciones, esto es, exponiéndolas al exterior.

- Controladora integrada
  - El sistema debe ser capaz de actuar como controladora de puntos de acceso Wireless así como de switches del mismo fabricante.
  - Esta funcionalidad no requerirá licencia adicional.
  - La gestión los APs y switches se hará desde la misma interfaz gráfica y CLI desde la que se gestiona el Firewall.
  - A nivel de Wifi las funcionalidades que al menos debe de realizar serán:

- Soporte de un amplio catálogo de APs, tanto indoor como outdoor, como switches, incluyendo rugged, sin que ninguna de esas funcionalidades requiera costes adicionales.
- Gestión completa de la seguridad de la plataforma wireless, incluyendo la protección frente a rogue APs, WIDS, monitorización (tanto de parámetros operativos como del medio radioeléctrico, incluyendo un análisis gráfico del espectro) y reporting
- Soporte para APs 802.3az WAVE2 y WiFi6
- Autenticación de SSID: WPA2-Personal, WPA2-Enterprise, WPA3 (SAE, SAE transition, Enterprise), Open. Múltiples PSK para WPA Personal.
- Soporte integrado o externo para portales cautivos, 802.1x, y preshared keys.
- Soporte para topologías wireless: Fast roaming, balanceo de carga entre APs, Wireless Mesh y bridging.
- Balanceo entre controladoras en caso de fallo.

- A nivel de Switch al menos deberá de realizar:
  - Funcionalidades configurables y monitorizables por puerto desde la consola centralizada (GUI y línea de comandos):
    - PoE (en los dispositivos compatibles)
    - DHCP blocking e IGMP snooping
    - STP (estado, BPDU, root guard)
    - LLDP, IGMP, sFlow y Dynamic ARP inspection (DAI)
    - Port mirroring
  - Políticas de seguridad por puerto:
    - 802.1x (en modos "basado en puerto" y "basado en MAC")
    - Restricción del tipo de trama permitida a través de los puertos IEEE 802.1Q
    - Soporte para RADIUS accounting
    - MAC authentication bypass configurable
    - EAP pass-through
  - Posibilidad de implementar políticas de NAC, empleando información de usuarios o información de los dispositivos detectada automáticamente (como el tipo de dispositivo o el sistema operativo, entre otros) para ubicar el tráfico en una VLAN específica o aplicar determinadas configuraciones de puertos.

- Servicio de Protección de Fugas de Información (DLP).
  - Soporte de los siguientes protocolos: HTTP/HTTPS, correo y mensajería instantánea.
  - Identificación y control de información corporativa sensible.
  - Análisis de los tipos de ficheros más utilizados (Microsoft Office y PDF).
  - Definición de patrones a nivel binario y de poder calcular el hash de los documentos a proteger para controlar su salida del perímetro.
  - Posibilidad de marcar documentos a proteger mediante una marca de agua identificable para evitar su salida de la organización.

Deberá disponer de la capacidad de hacer una extensión de puertos del firewall para mejorar la conectividad de la solución de seguridad con 48 bocas a 10Gb SFP+ y 4 enlaces a 100Gb SFP+ para realizar la separación física de toda la red.
Se valorarán especialmente soluciones que aporten también las siguientes características y funcionalidades adicionales:

- Fuente de alimentación redundante.
- Huella máxima: 1U.
- Licencias de usuario ilimitadas.
- Integración con soluciones de terceros, como:
  - Cloud pública: Google Cloud, Azure, AWS, Oracle y AliCloud.
  - Cloud privada: VMware (NSX y ESXi), Openstack, Kubernetes, Cisco ACI y Nuage.
  - Fuentes de identidad: Active Directory, LDAP y RADIUS/802.1x.
  - Fuentes de amenazas: Listado de IPs, dominios y hashs de malware.
- Balanceo de carga a granjas de servidores.
- Posibilidad de activación de funcionalidad de proxy explícito.
- Control de ancho de banda basado en IP, usuarios y/o aplicaciones.
- Inclusión en el propio equipo de un cliente iperf para realizar pruebas de carga de caudal sobre las líneas de comunicaciones.
- Disponer de certificaciones de Internet Computer Security Association (ICSA) en cortafuegos, IPSec, Network IPS, antivirus/antimalware, SSL-TLS.

6.1. GESTIÓN DE LOGS Y EVENTOS DE SEGURIDAD

Con objeto de centralizar y mantener los logs a largo plazo para cumplir con auditorías de seguridad de los cortafuegos solicitados, se solicita una plataforma de gestión y procesamiento especializada con las siguientes características:

- Equipo físico enrracable con capacidad de almacenamiento de al menos 4TB netos en al menos raid 1.
- Dispondrá de un cuadro de mando personalizable por usuario que accede al sistema con al menos la siguiente información: Aplicaciones más usadas, Aplicaciones de alto riesgo, Información general del sistema, Estado de los Interfaces, Logs relativos a las amenazas más observadas, Logs de filtrados URL o Recursos del sistema.
- Cuadro de mando de aplicaciones generado a partir de los logs, personalizable por usuario que permita disponer de información como los usuarios que más generan tráfico, las reglas de seguridad que más se usan, vulnerabilidades que más se han detectado y bloqueado, equipos que navegan hacia dominios maliciosos, virus detectados, información enviada a los servicios de sandboxing o host comprometidos en la red interna.
- Capacidad de uso de motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs recibidos se 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.
- Debe permitir realizar un análisis detallado del uso de red de los usuarios (tráfico enviado y recibido, sesiones, aplicaciones, amenazas, sitios web por lo que han navegado, políticas

aplicadas, interfaces, …).

- Múltiples usuarios de administración con diferentes perfiles de gestión administrativa basada en roles.
- Debe permitir el uso de informes predefinidos y la parametrización de informes a medida, en distintos idiomas y con gráficos configurables para ayudar a monitorizar y mantener identificados patrones de ataques, políticas de uso aceptable y a demostrar el cumplimiento de políticas.
- Deberá disponer de informes tanto de tipo técnico como de nivel ejecutivo, para Dirección, que permitan conocer el estado de uso de las redes de la organización, así como el nivel de seguridad y los ataques que se producen.
- Los informes deberán de poder generarse de forma automática y poderse programar en el tiempo, así como ser remitidos por correo electrónico.

- Permitir incorporar bibliotecas de indicadores de compromiso (IOC), para identificar dispositivos comprometidos, posibilitando una respuesta más ágil ante amenazas, o incluso la aplicación inmediata de acciones correctoras.
- Disponer de informes, entre otros, sobre anchos de banda consumidos por las diferentes aplicaciones/usuarios/sedes, informes sobre los orígenes y destinos geográficos de las amenazas detectadas, informes sobre análisis de comportamiento de tráfico observado que permita detectar equipos que tiene comprometido su seguridad.
- Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.
- Ejecución desde la plataforma de diferentes utilidades de diagnóstico, tales como: ping, traceroute y visor de logs.
- Según la naturaleza de los mismos, los informes se podrán obtener en formatos abiertos o en PDF.
- Arquitectura escalable que permita al dispositivo funcionar en modo colector o analizador, para optimizar el procesamiento de logs.
- Su inclusión en la guía CCN-STIC-105 de catálogo de productos STIC dentro de la familia de Sistemas de Gestión de Eventos de Seguridad.

7. GARANTÍA Y SOPORTE

La Escuela Andaluza de Salud Pública requiere colaboradores estratégicos que puedan ofrecer un servicio de soporte técnico especializado que garantice el óptimo funcionamiento de nuestra infraestructura tecnológica. Bajo la modalidad de 8 horas al día, 5 días a la semana (8x5), el servicio tiene como propósito principal asegurar la continuidad operativa, reducir riesgos y maximizar el rendimiento de nuestros sistemas críticos.

Todo el equipamiento suministrado deberá contar con una garantía de 3 años, que incluya:

- Sustitución por uno nuevo de igual o características superiores al retirado en caso de rotura.
- Soporte fabricante durante toda la duración del contrato. La Escuela Andaluza de Salud Pública gestionara estos soportes con los fabricantes.
- Actualizaciones de versiones de firmware (minor versions).
- Actualización de firmwares con nuevas funcionalidades (major versions).

Descripción del Servicio Requerido

El proveedor deberá aportar una combinación de experiencia técnica, herramientas avanzadas y un enfoque proactivo para la resolución de problemas. Entre los servicios necesarios se incluyen:

1. **Soporte Técnico Especializado:**

- Disponibilidad de un equipo altamente calificado para atender consultas técnicas y resolver incidentes de manera eficiente durante el horario especificado.
- Acceso a expertos que puedan abordar problemas complejos con rapidez y brindar asesoramiento técnico en tiempo real.

2. **Reemplazo de Hardware:**

- Garantía de continuidad operativa mediante un servicio de reemplazo de hardware defectuoso con tiempos de respuesta ajustados a la criticidad, desde el siguiente día hábil (NBD) hasta opciones más rápidas en áreas estratégicas.
- Disponibilidad de piezas originales y homologadas para asegurar la compatibilidad con nuestra infraestructura actual.

3. **Actualizaciones de Software y Firmware:**

- Acceso continuo a las últimas actualizaciones, incluyendo mejoras de rendimiento, parches de seguridad y nuevas funcionalidades del sistema.
- Capacidades para implementar dichas actualizaciones sin interrupciones en la operación.

4. **Diagnóstico Avanzado y Proactivo:**

- Herramientas automatizadas de monitoreo y diagnóstico que permitan identificar problemas potenciales antes de que afecten al sistema.
- Funcionalidades de alerta temprana para minimizar el impacto de posibles fallos.
- Generación de análisis predictivos basados en el comportamiento histórico y actual de los dispositivos.

5. **Gestión de Reportes:**

- Emisión periódica de reportes detallados sobre incidentes atendidos, acciones correctivas realizadas y recomendaciones para optimizar el rendimiento de la infraestructura.
- Acceso a un sistema en línea que permita visualizar reportes históricos y consultar información relevante en tiempo real.

6. Tiempos de Respuesta Garantizados:

- Compromiso de respuesta inmediata en función de la criticidad del incidente, con mecanismos claros para la resolución efectiva de problemas dentro de los plazos establecidos.
- Opciones de soporte in situ para incidentes críticos que requieran intervención directa en nuestras instalaciones.

7. Soporte Preventivo y Proactivo:

- Auditorías regulares y mantenimiento preventivo para garantizar la estabilidad de los sistemas.
- Propuestas de mejora continúa basadas en análisis detallados y datos predictivos.
- Perfil del Proveedor Ideal

Buscamos un socio tecnológico que reúna las siguientes cualidades:

- Certificaciones avanzadas en tecnologías de red y soporte técnico.
- Experiencia demostrable en proyectos similares, preferentemente con clientes de alta exigencia operativa.
- Acceso a herramientas de diagnóstico y resolución de problemas líderes en la industria.
- Capacidad para ofrecer soporte técnico y logístico tanto remoto como presencial, respaldado por acuerdos de nivel de servicio (SLA) sólidos.

8. FORMACIÓN

Es obligatoria la formación al personal técnico de la Escuela Andaluza de Salud Pública en la configuración y administración de los dispositivos objeto del suministro.

El mínimo de horas de formación será de 20, de forma online, dirigida a 5 empleados del la Escuela Andaluza de Salud Pública.

9. CARACTERÍSTICAS DEL SERVICIO

La empresa adjudicataria deberá incluir en la oferta la totalidad de los servicios necesarios para que el hardware quede alojado y totalmente actualizado. Será la Escuela Andaluza de Salud Pública, la que indicarán donde debe suministrarse el equipamiento.

En la oferta se deberá describir una planificación de los trabajos a realizar, con plazos y descripción lo más ajustada posible de las diferentes fases.

Como mínimo los servicios que deben incluirse son los siguientes:

- Recepción de los equipos y almacenamiento.
- Carga, transporte y descarga de los equipos.

- Alojamiento y actualización del software del nuevo equipamiento.

Se considerarán incluidos como parte del suministro a realizar, la actualización del firmware de los dispositivos, así como todo el material y accesorios necesarios para la correcta instalación de todo el equipamiento suministrado.

Se proveerá al adjudicatario del espacio necesario para emplazar todo el equipamiento, en los lugares en los que se tengan que almacenar.

9.1. CONDICIONES DEL SERVICIO

A continuación, se describen las condiciones generales del servicio:

- El equipamiento se suministrará en la modalidad de compra.
- El coste de la garantía, licencias y suscripciones de todos los productos que forman parte de la oferta estarán incluidos en la duración del contrato, y la documentación relacionada se deberá entregar al responsable del contrato de La Escuela Andaluza de Salud Pública.
- Quedan incluidos todos los trabajos a realizar, tanto en remoto como insitu, incluyendo los costes relacionados con los desplazamientos, dietas, repuestos y todo tipo de medios materiales necesarios para la reposición del equipamiento durante la vigencia del contrato.
- En caso de que el adjudicatario deba prestar servicio en remoto, este se realizará a través de conexiones seguras (VPN) habilitadas para tal efecto.
- El adjudicatario aportará los acuerdos y contratos necesarios con el fabricante para proporcionar los servicios requeridos en los términos indicados.

9.1.1. JEFE DE PROYECTO

El adjudicatario tendrá que designar un recurso que desempeñe la figura de jefe de Proyecto con las siguientes características y funciones.

- Interlocutor principal durante la fase de provisión (instalación, configuración, migración y puesta en servicio) del contrato para los servicios prestados por el adjudicatario aportando una visión global de los mismos. Será el responsable en fase de implantación, de dichos servicios, controlando la calidad de acuerdo a los compromisos adquiridos y en general, de impulsar la evolución de los servicios de implantación dentro de los parámetros establecidos en el contrato. No se requiere de dedicación 100% pero tendrá que ser plantilla del adjudicatario y su puesto de trabajo estará ubicado en las instalaciones del adjudicatario a no más de 150 Km de la Escuela Andaluza de Salud Pública, teniéndose que desplazar a las instalaciones siempre que sea necesario. No se permite la subcontratación de este servicio.
- Será el responsable de la planificación y seguimiento global de la implantación coordinando los equipos de trabajo involucrados.
- Coordinación interna con los responsables la Escuela Andaluza de Salud Pública
- Definición y ejecución de procedimientos de actuación para garantizar la correcta provisión de los servicios.
- Identificación de problemas en la implantación, siendo responsable de la gestión de los mismos.

9.2. PLAZO MÁXIMO DE SUMINISTRO

Se establece un plazo máximo de 3 meses desde la formalización del contrato para el suministro, instalación, migración de servicios, configuración y puesta en explotación del equipamiento ofertado.

10. DOCUMENTACIÓN A PRESENTAR

Las ofertas deben adecuarse a las características mínimas de servicio fijadas en este Pliego de Prescripciones Técnicas. Las ofertas deberán presentarse de forma clara, fácilmente legible y detallando las características técnicas de los elementos objeto del contrato.

Con el fin de comprobar el cumplimiento de los requisitos mínimos, de obligado cumplimiento, establecidos en el presente documento, la oferta deberá incluir memoria técnica en la que se detalle el número, marca y modelo de cada dispositivo ofertado, las características técnicas oficiales de cada uno de ellos y el plan de cumplimiento de los servicios asociados al suministro requeridos.

Para facilitar la comprobación de los requisitos técnicos requeridos en el presente documento, el licitador deberá incluir obligatoriamente en la memoria técnica la documentación técnica oficial de los productos que oferte, junto con documento anexo en el que indique, para cada característica técnica requerida, la referencia a la documentación técnica oficial del fabricante en la que se especifique el cumplimiento de dicho requisito. La inclusión de dicho documento es requisito obligatorio. La ausencia del mismo en la oferta podrá dar lugar a la exclusión de la misma.

10.1. PLAN DE IMPLANTACIÓN Y PLAN DE MIGRACIÓN Y COEXISTENCIA

Junto con la Memoria técnica, se deberá presentar:

- **Plan de Implantación**: Documento que describe las actividades y tareas necesarias para desplegar los servicios ofertados.
- **Plan de Migración**: Documento que describe las actividades y tareas necesarias para migrar los servicios actuales a los nuevos que haya ofertado.

Estos documentos deberán cubrir todas las tareas y actuaciones necesarias para la implantación definitiva de los servicios correspondientes a este contrato y serán vinculantes durante la duración del contrato.

El plan de migración incluirá también la puesta en producción de los nuevos servicios cuando no existieran servicios actuales previos.

Un servicio se considera totalmente implantado y en producción cuando, tras quedar documentada por el adjudicatario la entrega del mismo, se valide la conformidad de los trabajos por parte del responsable del Contrato de la Escuela Andaluza de Salud Pública atendiendo a lo establecido en el pliego de prescripciones técnicas, mediante acta levantada al efecto.

Se deberá hacer mención a los servicios descritos en el apartado “situación actual” y a la solución de continuidad, desde el primer día del plazo de implantación, migración y coexistencia, fecha en la que empieza a proveer los servicios el adjudicatario del contrato hasta finalizada la migración a los nuevos servicios.

10.1.1. PLAN DE IMPLANTACIÓN

El objetivo del Plan de Implantación es definir las actividades y tareas necesarias para el despliegue de los servicios ofertados de forma compatible con el funcionamiento de los servicios actuales, garantizando la continuidad del servicio durante el proceso de implantación.

Requisitos

Además de los requisitos mencionados, el Plan de Implantación debe incluir los siguientes requisitos:

- Seguridad: El plan debe garantizar la seguridad de los servicios durante todo el proceso de implantación.
- Reparación y mantenimiento: El plan debe definir las acciones que se realizarán para reparar o mantener los servicios en caso de que se produzcan fallos o incidencias durante el proceso de implantación.
- Formación: El plan debe definir las acciones que se realizarán para formar a los usuarios de los servicios en el uso de los nuevos sistemas.

Estructura

La estructura del Plan de Implantación debe ser la siguiente:

- Introducción: Esta sección debe incluir una descripción general del plan, incluyendo los objetivos, requisitos, estructura y metodología de elaboración del mismo.
- Análisis de la situación actual: Esta sección debe describir la situación actual de los servicios que se van a implantar, incluyendo los sistemas, infraestructura y procesos actuales.
- Diseño de la implantación: Esta sección debe definir el diseño de la implantación, incluyendo la infraestructura, los sistemas y los procesos necesarios para la prestación de los servicios.
- Pruebas: Esta sección debe definir las pruebas que se realizarán para validar el correcto funcionamiento de los servicios tras la implantación.
- Puesta a punto: Esta sección debe definir las acciones que se realizarán para ajustar los parámetros de los servicios tras la implantación.
- Plazos de ejecución: Esta sección debe definir los plazos de ejecución de cada una de las actividades.
- Replanteo del servicio: Esta sección debe definir el procedimiento para el replanteo del servicio en caso de que sea necesario modificar el plan inicial.
- Planificación temporal para la instalación de las herramientas de monitorización y gestión: Esta sección debe definir la planificación temporal para la instalación de las herramientas de monitorización y gestión de los servicios.
- Gestión de riesgos: Esta sección debe definir los riesgos asociados al proceso de implantación y las acciones que se realizarán para mitigarlos.

Comprobación

El Plan de Implantación será objeto de informe técnico por los servicios técnicos de la Escuela Andaluza de Salud Pública quienes comprobarán que se ajustan al presente pliego. Específicamente la comprobación se centrará en los siguientes aspectos:

- Completitud: El plan debe incluir toda la información necesaria para su correcta ejecución.
- Especificidad: El plan debe ser lo suficientemente específico para permitir su seguimiento y control.
- Realismo: El plan debe ser realista y alcanzable dentro de los plazos y recursos disponibles.
- Calidad: El plan debe estar bien documentado y redactado de forma clara y concisa.
- Gestión de riesgos: El plan debe identificar y mitigar los riesgos asociados al proceso de implantación.

10.1.2. PLAN DE MIGRACIÓN Y COEXISTENCIA

El objetivo del Plan de Migración y Coexistencia es definir las actividades y tareas necesarias para migrar los servicios actuales a los nuevos sistemas, garantizando la continuidad del servicio durante todo el proceso.

Además, el Plan de Migración y Coexistencia debe incluir los siguientes requisitos:

- Seguridad: El plan debe garantizar la seguridad de los datos y sistemas durante todo el proceso de migración.
- Reparación y mantenimiento: El plan debe definir las acciones que se realizarán para reparar o mantener los servicios en caso de que se produzcan fallos o incidencias durante el proceso de migración.
- Formación: El plan debe definir las acciones que se realizarán para formar a los usuarios de los servicios en el uso de los nuevos sistemas.

Estructura

La estructura del Plan de Migración y Coexistencia debe ser la siguiente:

- Introducción: Esta sección debe incluir una descripción general del plan, incluyendo los objetivos, requisitos, estructura y metodología de elaboración del mismo.
- Análisis de la situación actual: Esta sección debe describir la situación actual de los servicios que se van a migrar, incluyendo los sistemas, infraestructura y procesos actuales.
- Diseño de la migración: Esta sección debe definir el diseño de la migración, incluyendo la infraestructura, los sistemas y los procesos necesarios para la migración de los servicios.
- Pruebas: Esta sección debe definir las pruebas que se realizarán para validar el correcto funcionamiento de los servicios tras la migración.
- Puesta a punto: Esta sección debe definir las acciones que se realizarán para ajustar los parámetros de los servicios tras la migración.
- Plazos de ejecución: Esta sección debe definir los plazos de ejecución de cada una de las actividades.
- Replanteo del servicio: Esta sección debe definir el procedimiento para el replanteo del servicio en caso de que sea necesario modificar el plan inicial.
- Gestión de riesgos: Esta sección debe definir los riesgos asociados al proceso de migración y coexistencia y las acciones que se realizarán para mitigarlos.

Comprobación

El Plan de Migración y Coexistencia será objeto de informe técnico por los servicios técnicos de la Escuela Andaluza de Salud Pública quienes comprobarán que se ajustan al presente pliego. Específicamente la comprobación se centrará en los siguientes aspectos:

- Completitud: El plan debe incluir toda la información necesaria para su correcta ejecución.
- Especificidad: El plan debe ser lo suficientemente específico para permitir su seguimiento y control.
- Realismo: El plan debe ser realista y alcanzable dentro de los plazos y recursos disponibles.
- Calidad: El plan debe estar bien documentado y redactado de forma clara y concisa.
- Gestión de riesgos: El plan debe identificar y mitigar los riesgos asociados al proceso de migración y coexistencia.

11. IMPORTE DE LICITACIÓN Y FACTURACIÓN

El importe máximo de la licitación es de 176.250 € más 37.012,50 € en concepto del 21% de IVA, lo que supone un total de 213.262,50 € (doscientos trece mil doscientos sesenta y dos euros, con cincuenta céntimos).

El valor estimado del contrato de suministro es de 213.262,50€.

La siguiente tabla resume las imputaciones anuales previstas:

Anualidades	Base	IVA	Total
2025	176.250,00 €	37.012,50 €	213.262,50 €

No obstante, si la adjudicación y formalización del contrato se efectuase con posterioridad a la fecha prevista, se propone que el órgano de contratación autorice a la por persona responsable a quién competa, al objeto de que directamente efectúe el reajuste de su financiación, sin que ello requiera ser nuevamente aprobado.

La facturación se articulará de la siguiente forma:

Se emitirá una única factura una vez realizado el suministro de todo el equipamiento en las condiciones establecidas en este Pliego de Prescripciones Técnicas y tras la verificación de la correcta ejecución por el responsable del contrato.

Conocido y aceptado en su totalidad, en Granada, a fecha de la firma electrónica

Fdo. Blanca del Rocío Botello Díaz

Directora Gerente de la Escuela Andaluza de Salud Pública.

BOTELLO DIAZ BLANCA DEL ROCIO - 48921221Z

Firmado digitalmente por BOTELLO DIAZ BLANCA DEL ROCIO - 48921221Z
DN: C=ES, SERIALNUMBER=IDCES-48921221Z, G=BLANCA DEL ROCIO, SN=BOTELLO DIAZ, CN=BOTELLO DIAZ BLANCA DEL ROCIO - 48921221Z
Razón: Mi firma en este documento representa mi aceptación de los términos definidos
Ubicación:
Fecha: 2025.09.23 08:49:09+02'00'
Foxit PDF Reader Versión: 2025.2.0