

MANTENIMIENTO Y EVOLUCIÓN TECNOLÓGICA DE HARDWARE Y SOFTWARE DE RED.

PLIEGO DE PRESCRIPCIONES TÉCNICAS (PPT). EXP 46/24

OBJETO:

El objeto del presente contrato consiste en la prestación del servicio de mantenimiento y evolución tecnológica del parque de dispositivos hardware y software de red de la Diputación Foral de Álava y entidades:

- Diputación Foral de Álava (en adelante DFA)
- Instituto Foral de Bienestar Social (en adelante IFBS)
- Indesa
- Juntas Generales de Álava (en adelante JJGG)
- Artium

Dicho parque está constituido por dispositivos hardware y software de los siguientes fabricantes:

- Cisco
- Checkpoint
- F5
- Microfocus
- Fortinet



1. Antecedentes

La DFA y entidades disponen de redes constituidas por dispositivos hardware y software de los siguientes fabricantes:

- Cisco (switches, routers, Access points, firewalls, ...)
- Checkpoint (firewalls)
- F5 (balanceadores/portales de aplicaciones/firewalls)
- Microfocus (software de gestión)
- Fortinet (firewalls)

Estos dispositivos hardware y software han sido adquiridos en diferentes momentos y a distintos proveedores, típicamente con garantía de compra por tres años. Algunos de ellos han alcanzado, o están próximos a alcanzar, su fecha de “end of support” por parte del fabricante.

La DFA y entidades desean disponer de un servicio de mantenimiento hardware y software para todos sus dispositivos y software de red con un único proveedor.

También desean la evolución tecnológica de los dispositivos más críticos que han alcanzado, o están próximos a alcanzar, su fecha de “end of support” por parte del fabricante.

Asimismo, desean disponer de un servicio de soporte para consultas relacionadas con estos dispositivos hardware y software.

Para ello, se ha venido contratando el servicio de mantenimiento de su parque de dispositivos hardware y software de red por periodos de tres años. El 30-06-2024, finaliza el actual contrato de mantenimiento y la DFA y entidades desean contratar uno nuevo por otro periodo de tres años.

2. Equipamiento objeto del contrato

En el Anexo “Hardware y software a mantener” figura el listado de equipamiento objeto del contrato. Por motivos de seguridad de la DFA y las entidades, en el presente pliego no se publica dicho anexo. Los interesados en el proceso de licitación, deberán solicitarlo de las fuentes en la dirección de correo electrónico sectecsergen@araba.eus indicando:

- Empresa solicitante
- Nombre del contacto
- Correo electrónico
- Número de teléfono del contacto

Se deberá firmar el correspondiente compromiso de confidencialidad.

3. Productos y/o servicios a contratar

El adjudicatario del presente contrato deberá proporcionar los siguientes servicios sobre los dispositivos hardware y software de red que se especifican en el Anexo:

3.1. Servicio de “ventanilla única”

- Exclusivamente para los dispositivos del fabricante Cisco cuya fecha de “fin de garantía de compra” es posterior al 30-06-2024.
- Desde el 01-07-2024 hasta la fecha de “fin de garantía de compra”.
- En caso de avería, tramitación de la garantía del equipo con el proveedor que lo suministró.

3.2. Servicio de mantenimiento hardware y software

- Para el resto de dispositivos y software, desde el 01-07-2024 hasta el 30-06-2027.
- Como excepción, para los equipos actuales objeto del servicio de evolución tecnológica descrito en el apartado 3.4, sólo será necesario prestar este servicio hasta el momento en que sean sustituidos por equipos nuevos.
- Para los dispositivos del fabricante Cisco cuya fecha de “fin de garantía de compra” es posterior al 30-06-2024, desde la fecha de “fin de garantía de compra” hasta el 30-06-2027
- Se ofertará siempre el mantenimiento del propio fabricante o compartido entre el fabricante y el partner, salvo para aquellos equipos que alcancen su fecha de End of Support (EoS) por parte del fabricante durante la vigencia del contrato. En estos casos el mantenimiento lo deberá prestar el adjudicatario por sus propios medios a partir de la fecha de EoS por parte del fabricante.
- Atención 8x5
- Reposición hardware en 24 horas “Next Bussiness Day” en las dependencias del Centro de Cálculo de Álava, sito en Plaza de la Provincia, s/n.
- Suministro de nuevas versiones que introduzcan nuevas funcionalidades y/o corrijan problemas.
- Suscripción del fabricante para el disfrute de las funcionalidades software indicadas.
- Posibilidad de abrir casos de soporte con el fabricante.

- Los equipos averiados deberán ser sustituidos por equipos idénticos o superiores del mismo fabricante.

3.3. Servicio de soporte para consultas

Servicio de Soporte para resolución de dudas o consultas de networking en general y relacionadas con los dispositivos de red detallados en el Anexo y los nuevos equipos que se propongan como evolución tecnológica (apartado 3.4).

- Para todos los dispositivos y software desde el 01-07-2024 hasta el 30-06-2027.
- Atención 8x5
- Por medios telemáticos.

3.4. Servicio de evolución tecnológica

Algunos de los dispositivos de red objeto del contrato, han alcanzado, o están próximos a alcanzar, su fecha de “end of support” por parte del fabricante. Varios de ellos son especialmente críticos y la falta de mantenimiento por parte del fabricante sería incompatible con las mínimas garantías de disponibilidad y evolución que estos sistemas requieren.

En estos casos, se propone un servicio de evolución tecnológica a otros equipos más modernos, que presten las mismas funcionalidades que los actuales o superiores, ofrezcan más capacidades y tengan suficiente recorrido dentro del ciclo de vida del fabricante.

- Se deberá suministrar, instalar y configurar los nuevos equipos de forma que queden plenamente operativos e integrados en la red de la DFA con, al menos, las mismas funcionalidades que están prestando los equipos actuales.
- Se deberá actualizar los nuevos equipos a la última versión de software que en el momento de la implantación esté disponible.
- La evolución se deberá realizar antes del 31-12-2024
- Los equipos nuevos estarán cubiertos por el servicio de mantenimiento hardware y software descrito en el apartado anterior desde el momento de su implantación hasta el fin del contrato.
- Los equipos actuales deberán ser desinstalados. El adjudicatario podrá disponer de los equipos actuales sustituidos.

En concreto este servicio debe prestarse para los siguientes equipos:

3.4.1. Firewalls externos

En el anexo de “Hardware y software a mantener”, en la solapas “DFA-Checkpoint” y “JJGG-Checkpoint”, los equipos identificados como:

- Firewall perimetral, Nodos 1 y 2

Deberán ser evolucionados a un sistema de firewall compuesto por dos nodos de firewall en formato físico. Los nuevos nodos deberán integrarse con la consola de firewall perimetral ya disponible, cuyo detalle se puede ver en el anexo “Hardware y software a mantener”, en la solapa “DFA-Checkpoint”, apartado “firewall perimetral”. Los dos nuevos nodos, junto con la consola existente, formarán un conjunto en alta disponibilidad.

Cada nodo de firewall debe disponer , al menos, de las siguientes capacidades:

- Puerto de consola
- 1 puerto 10/100/1000 Base-T de sincronismo
- 1 puerto 10/100/1000 Base-T de gestión
- 8 puertos 10/100/1000 Base-T de servicio
- Capacidad de ampliación con un módulo de red de puertos adicionales
- Fuentes de alimentación redundantes
- 1 disco de 480 GB SSD
- 16 Gb de memoria
- Rendimiento (medido en condiciones empresariales)
 - Firewall 26 Gbps
 - IPS 19 Gbps
 - NGFW (con firewall, application control e IPS con logeo activado): 13,4 Gbps
 - Thread prevention (con firewall, application control, IPS, URL filtering, Antivirus, Antibot y con protección de día cero, con logeo activado) 5,8 Gbps
- Rendimiento (medido en condiciones de laboratorio)
 - Firewall 38 Gbps
- Integración con AD, LDAP y Radius

- Gestión en dos planos: control de acceso (reglas de firewall, control de aplicaciones, ...) y seguridad (IPS, antivirus, ...)
- Posibilidad de definir una política por capas (conjunto de reglas)
- Funcionalidades de:
 - Firewall
 - VPN (IPSEC y SSL)
 - Identity awareness
 - Content awareness
 - Application control
 - Intrusion prevention system
 - URL filtering
 - Antivirus, antibot y antispam
 - Seguridad DNS
- Capacidad para incluir, mediante subscripciones adicionales, funcionalidades de:
 - SDWAN
 - Protección IoT
 - Thread prevention y thread extraction

Por motivos de cumplimiento del Esquema Nacional de Seguridad, y para dotar de una doble barrera de firewall de diferentes fabricantes, la solución propuesta para el firewall perimetral deberá ser de diferente fabricante que la propuesta para el firewall interno (detallado más adelante).

- Firewall de Casa Cultura

Deberá ser evolucionado a un sistema de firewall compuesto por un nodo de firewall en formato físico. Por facilidad de gestión y uniformidad en las políticas, deberá poder gestionarse desde la misma consola centralizada que los firewalls perimetrales descritos anteriormente.

El nodo de firewall debe disponer , al menos, de las siguientes capacidades:

- Puerto de consola
- 1 puerto 10/100/1000 Base-T de gestión

- 5 puertos 10/100/1000 Base-T de servicio
- 1 disco de 240 GB SSD
- 16 Gb de memoria
- Enrackable o con kit de enrackado.
- Rendimiento (medido en condiciones empresariales)
 - Firewall 3,6 Gbps
 - IPS 3,3 Gbps
 - NGFW (con firewall, application control e IPS con logeo activado): 3 Gbps
 - Thread prevention (con firewall, application control, URL filtering, IPS, Antivirus, Antibot y con protección de día cero, con logeo activado) 1,5 Gbps
- Rendimiento (medido en condiciones de laboratorio)
 - Firewall 4 Gbps
- Integración con AD, LDAP y Radius
- Gestión en dos planos: control de acceso (reglas de firewall, control de aplicaciones, ...) y seguridad (IPS, antivirus, ...)
- Posibilidad de definir una política por capas (conjunto de reglas)
- Funcionalidades de:
 - Firewall
 - VPN (IPSEC y SSL)
 - Identity awareness
 - Content awareness
 - Application control
 - Intrusion prevention system
 - URL filtering
 - Antivirus, antibot y antispam
 - Seguridad DNS

- Firewall de Juntas Generales

Deberá ser evolucionado a un sistema de firewall compuesto por un nodo de firewall en formato físico. Por facilidad de gestión y uniformidad en las políticas, deberá poder gestionarse desde la misma consola centralizada que los firewalls perimetrales descritos anteriormente.

El nodo de firewall debe disponer , al menos, de las siguientes capacidades:

- Puerto de consola
- 1 puerto 10/100/1000 Base-T de sincronismo
- 1 puerto 10/100/1000 Base-T de gestión
- 8 puertos 10/100/1000 Base-T de servicio
- Capacidad de ampliación con un módulo de red de puertos adicionales
- Fuentes de alimentación redundantes
- 1 disco de 240 GB SSD
- 8 Gb de memoria
- Rendimiento (medido en condiciones empresariales)
 - Firewall 9 Gbps
 - IPS 4,6 Gbps
 - NGFW (con firewall, application control e IPS con logeo activado): 3,7 Gbps
 - Thread prevention (con firewall, application control, URL filtering, IPS, Antivirus, Antibot y con protección de día cero, con logeo activado) 1,8 Gbps
- Rendimiento (medido en condiciones de laboratorio)
 - Firewall 17,5 Gbps
- Integración con AD, LDAP y Radius
- Gestión en dos planos: control de acceso (reglas de firewall, control de aplicaciones, ...) y seguridad (IPS, antivirus, ...)
- Posibilidad de definir una política por capas (conjunto de reglas)
- Funcionalidades de:

- Firewall
- VPN (IPSEC y SSL)
- Identity awareness
- Content awareness
- Application control
- Intrusion prevention system
- URL filtering
- Antivirus, antibot y antispam
- Seguridad DNS

3.4.2. Firewall interno

En el anexo de “Hardware y software a mantener”, en la solapa “DFA-Cisco CPD”, los equipos identificados como:

- Firewall interno

Deberán ser evolucionados a un sistema de firewall compuesto por dos nodos de firewall en formato físico. Los nodos formarán un conjunto en alta disponibilidad.

Cada nodo de firewall debe disponer , al menos, de las siguientes capacidades:

- Puerto de consola
- 1 puerto 2,5/1 GE RJ45 de HA
- 1 puerto 1 GE RJ45 de gestión
- 16 puertos GE RJ45 de servicio
- 8 puertos GE SFP slots
- 4 puertos 10GE/GE SFP+/SFP slots
- 4 puertos 25GE/10GE SFP28/SFP+ slots
- Equipado con 2 x SFP SX
- Fuentes de alimentación redundantes

- 2 discos de 480 GB
- TPM para la generación, almacenamiento y autenticación de claves criptográficas
- Rendimiento (medido en condiciones empresariales)
 - IPS (Con logeo activado) 26 Gbps
 - NGFW (con firewall, application control e IPS, con logeo activado): 22 Gbps
 - Thread protection (con firewall, application control, IPS y protección antimalware, con logeo activado) 20 Gbps
- Rendimiento (medido en condiciones de laboratorio)
 - Firewall 164 Gbps
- Integración con AD
- Funcionalidades de:
 - Firewall
 - VPN (IPSEC y SSL)
 - Identity awareness
 - Application control
 - Intrusion prevention system
 - URL filtering
 - Antimalware (incluyendo servicio sandbox en nube)
 - Seguridad DNS
 - SDWAN
 - Base de datos de servicios en Internet
 - Base de datos de geolocalización de IP's en internet

Por motivos de cumplimiento del Esquema Nacional de Seguridad, y para dotar de una doble barrera de firewall de diferentes fabricantes, la solución propuesta para el firewall interno deberá ser de diferente fabricante que la propuesta para el firewall perimetral (detallado anteriormente).

3.4.3. Equipos de Core de CPD

En el anexo de “Hardware y software a mantener”, en la solapa “DFA-Cisco CPD”, los equipos identificados como:

- Equipo sl4002-ccasa-cpd (modelo N9K-C93120TX)
- Equipo sl4003-ccasa-cpd (modelo N9K-C93120TX)
- Equipo sl4005-ha-cpd (modelo N9K-C93120TX)
- Equipo sl4006-ha-cpd (modelo N9K-C93120TX)
- Equipo ss4000-ccasa-cpd (modelo N9K-C9336PQ)
- Equipo ss4001-ha-cpd (modelo N9K-C9336PQ)
- Equipo APIC-N1 (modelo APIC-SERVER-M2)
- Equipo APIC-N2 (modelo APIC-SERVER-M2)
- Equipo APIC-N3 (modelo APIC-SERVER-M2)

Estos equipos, conforman un fabric de ACI junto con otros equipos que se mantienen en la instalación ya que todavía les queda recorrido en su ciclo de vida. En el anexo de “Hardware y software a mantener”, en la solapa “DFA-Cisco CPD”, bajo el epígrafe de “Core de red”, pueden comprobarse todos los equipos que constituyen el fabric de ACI. Por este motivo, estos equipos deben ser evolucionados a otros equipos nuevos compatibles con los equipos que se mantienen en la instalación.

En concreto, deberán ser evolucionados a los siguientes equipos:

- Equipo sl4002-ccasa-cpd (modelo N9K-C93120TX) -> Cisco Nexus 93216TC-FX2 Switch
- Equipo sl4003-ccasa-cpd (modelo N9K-C93120TX) -> Cisco Nexus 93216TC-FX2 Switch
- Equipo sl4005-ha-cpd (modelo N9K-C93120TX) -> Cisco Nexus 93216TC-FX2 Switch
- Equipo sl4006-ha-cpd (modelo N9K-C93120TX) -> Cisco Nexus 93216TC-FX2 Switch
- Equipo ss4000-ccasa-cpd (modelo N9K-C9336PQ) -> Cisco Nexus 93600CD-GX Switch
- Equipo ss4001-ha-cpd (modelo N9K-C9336PQ) -> Cisco Nexus 93600CD-GX Switch
- Equipo APIC-N1 (modelo APIC-SERVER-M2) -> Cisco APIC-SERVER-M4
- Equipo APIC-N2 (modelo APIC-SERVER-M2) -> Cisco APIC-SERVER-M4

- Equipo APIC-N3 (modelo APIC-SERVER-M2) -> Cisco APIC-SERVER-M4

Todos los equipos nuevos se suministrarán con fuentes de alimentación redundantes.

4. Modo de ejecución

➤ **Entrega del suministro:**

Los productos deberán entregarse en las instalaciones de CCASA sitas en Plaza de la provincia, s/n, 01001 Vitoria-Gasteiz.

Las licencias o subscripciones deberán entregarse a CCASA o registrarse en las User Accounts de la DFA en los diferentes fabricantes.

➤ **Servicio de evolución tecnológica:**

Para el servicio de evolución tecnológica, deberá dedicarse, al menos:

- Un ingeniero certificado en Cisco para el servicio de evolución tecnológica de equipos de Core de CPD.
- Un ingeniero certificado en el fabricante de firewall propuesto para el servicio de evolución tecnológica de firewall perimetral.
- Un ingeniero certificado en el fabricante de firewall propuesto para el servicio de evolución tecnológica de firewall interno.

Se admite un mismo Ingeniero con varias de las certificaciones requeridas.

➤ **Plazos para el suministro e instalación:**

Todos los equipos objeto del servicio de evolución tecnológica deberán quedar entregados, instalados, configurados y operativos antes del 31-12-2024.