Perfeccionamiento de la arquitectura de protección perimetral de la Consejería de Conocimiento, Investigación y Universidad

Expediente: CONTR 2018 0000070879

Pliego de Prescripciones Técnicas.

El presente pliego de prescripciones técnicas particulares, propuesto por el jefe del servicio de informática con fecha 30 de octubre de 2018, ha sido aprobado para su utilización en el expediente de referencia por resolución de este órgano de la fecha indicada en la diligencia de verificación de firma electrónica.

La persona titular de la Secretaría General Técnica.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 1 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

ÍNDICE:

1. Introducción....3
2. Objeto....4
3. Alcance....4
4. Consideraciones previas de carácter general....5
4.1. Etiquetado de los dispositivos....5
4.2. Documentación a entregar....5
5. Especificaciones técnicas de los dispositivos objeto de esta contratación....6
5.1. Observaciones generales relativas a todos los dispositivos....6
5.2. Especificaciones técnicas de los cortafuegos (incluidos en el LOTE I)....7
5.2.1. Consideraciones previas relativas a los cortafuegos....7
5.2.2. Especificaciones técnicas del modelo XL....11
5.2.3. Especificaciones técnicas del modelo L....12
5.2.4. Especificaciones técnicas del modelo M....12
5.2.5. Especificaciones técnicas del modelo S....13
5.3. Especificaciones técnicas de la plataforma de gestión centralizada (incluida en el LOTE I)....13
5.4. Especificaciones técnicas de la herramienta de gestión de logs (incluida en el LOTE I)....14
5.5. Especificaciones técnicas del firewall a nivel de aplicación (WAF) (incluido en el LOTE I)....16
5.6. Especificaciones técnicas de los switches o conmutadores de red (incluidos en el LOTE II)....18
5.7. Especificaciones técnicas de los transceptores y el cableado de conexión (incluidos en el LOTE II)....21
6. Condiciones de la garantía....23
7. Otras especificaciones técnicas de carácter normativo....25
7.1. Consideraciones sobre normalización....25
7.2. Cumplimiento de normas medioambientales, ergonómicas y otras....25
8. Cumplimiento de la normativa en materia de protección de datos de carácter personal y el ENS....26
8.1. Seguridad de los sistemas y cumplimiento del ENS....26
8.2. Confidencialidad e integridad de la información y protección de datos de carácter personal....26
9. Propiedad intelectual....27
10. Presupuesto detallado....27
Anexo I. Modelos descatalogados no susceptibles de ser ofertados....29
Anexo II. Especificaciones técnicas de los dispositivos....31
Anexo III: Glosario de términos, acrónimos y abreviaturas....38
Anexo IV. Procedimiento de inventariado de bienes no homologados....41
1. Objeto....41
2. Alcance....41
3. Requisitos mínimos que debe cumplir el proveedor....41
4. Secuencia de actividades para el inventariado de bienes informáticos....41
5. Procedimiento de etiquetado de los equipos por parte del proveedor....42
6. Procedimiento de inserción de datos en CRIJA por parte del proveedor....44
7. Verificación del etiquetado....44
8. Entrega y validación del etiquetado....45
Anexo V. Sedes incluidas en la Primera Fase del Programa de Securización Perimetral de CCIU....46

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 2 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

1. Introducción.

La Consejería de Conocimiento, Investigación y Universidad (en adelante CCIU) de la Junta de Andalucía se crea el pasado 6 de junio de 2018.[1] Esta nueva Consejería mantiene gran parte de los centros directivos pertenecientes a la extinta Consejería de Economía y Conocimiento (en adelante CEC).[2] Asimismo, las actualmente denominadas Delegaciones Territoriales de Conocimiento y Empleo (en adelante DDTT), a las que se adscriben los servicios periféricos tanto de la Consejería de Empleo Empresa y Comercio (en adelante CEEC), como de la actual CCIU, dependen orgánicamente de esta última Consejería.[3]

Todas las organizaciones anteriores cuentan con sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Esquema Nacional de Seguridad (en adelante ENS),[4] Es precisamente el art. 22 del RD 3/2010 donde se establece la obligatoriedad de proteger el perímetro de los sistemas a interconectar, en particular si se utilizan redes públicas, total o parcialmente, y de analizar los riesgos derivados de la interconexión de los sistemas, controlando además su punto de unión. En esta línea, habría que añadir que es voluntad de CCIU obtener próximamente la **Certificación de Conformidad** regulada en el ENS, certificación obligatoria para los sistemas de categoría media y alta y voluntaria para los sistemas clasificados de categoría básica.

En la actualidad, ni las sedes principales de las DDTT, ni otras sedes menores distribuidas por todo el territorio andaluz con acceso a Internet (como edificios secundarios, archivos provinciales, etc.), cuentan con dispositivos de seguridad perimetral desplegados y configurados *ex professo* para esta finalidad. Siendo la cobertura general que presta la Red Corporativa de la Junta de Andalucía (en adelante RCJA) la única defensa perimetral con la que cuentan estas sedes.

Por otra parte, la sede de los servicios centrales de CCIU (en adelante SSCC) en la Isla de la Cartuja y su Centro de Proceso de Datos (en adelante CPD), ubicado en el municipio de Tomares (Sevilla) en las instalaciones de la empresa pública SANDETEL, si bien, cuentan con cortafuegos destinados a su seguridad perimetral, estos dispositivos se encuentran descatalogados y en un estado de obsolescencia tecnológica tal que hacen necesaria su inmediata renovación. Esta situación, unida a la necesidad de administrar de forma conjunta la seguridad perimetral de toda la Consejería, ha motivado la decisión de incluir el CPD y la sede de los SSCC en esta primera fase del programa de mejora de la seguridad perimetral de CCIU.

---

1 Decreto de la Presidenta 5/2018, de 6 de junio, de la Vicepresidencia y sobre reestructuración de Consejerías (BOJA extraordinario nº 4 de 06/06/2018).
2 Decreto 108/2018, de 19 de junio, por el que se regula la estructura orgánica de la Consejería de Conocimiento, Investigación y Universidad (BOJA nº 120 de 22/06/2018).
3 Decreto 107/2018, de 19 de junio, por el que se regula la estructura orgánica de la Consejería de Economía, Hacienda y Administración Pública y se modifica el Decreto 342/2012, de 31 de julio, por el que se regula la organización territorial provincial de la Administración de la Junta de Andalucía (BOJA nº 120 de 22/06/2018).
4. RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y su modificación mediante el RD 951/2015, de 23 de octubre según lo previsto en el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 3 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

2. Objeto.

El presente Pliego de Prescripciones Técnicas (en adelante PPT) describe el diseño de la solución adoptada y establece los requisitos mínimos que deberán cumplir los dispositivos destinados a perfeccionar la Arquitectura de Protección Perimetral (en adelante APP) de CCIU, incluyendo sus DDTT y el resto de sedes que dependen de éstas con acceso a Internet. Asimismo, se incluyen algunas de las obligaciones a asumir por la empresa contratista en aras del cumplimiento de la normativa vigente.

3. Alcance.

El alcance de este PPT comprende la adquisición de los dispositivos de red y el software en su definición más amplia, necesarios para implementar una eficaz APP de nueva generación en las instalaciones de CCIU y las sedes de sus DDTT. Siguiendo la dinámica establecida en la nueva Ley de Contratos del Sector Público,[5] se ha dividido el conjunto de suministros a adquirir en dos lotes distintos:

Lote I: Dispositivos de seguridad perimetral.

- Dos cortafuegos de gama media-alta (para configurar en alta disponibilidad) destinados al CPD de CCIU ubicado en el edificio ZOCO en Tomares (Sevilla).
- Un total de 18 cortafuegos de gama media. Dos para cada una de las ocho sedes principales de las DDTT (para configurar en alta disponibilidad) y dos más para la sede principal de los SSCC de CCIU en el edificio Kepler (en la Isla de la Cartuja, Sevilla).
- Un total de 18 cortafuegos de gama media-baja. Dos para cada una de las ocho sedes secundarias dependientes de las DDTT (sedes con entre 20 y 80 usuarios) distribuidas por todo el territorio andaluz (también para configurar en alta disponibilidad) y dos más para el laboratorio de ciberseguridad del Servicio de Informática de CCIU y el stock de emergencia contemplado en el Protocolo de respuesta rápida ante incidentes de ciberseguridad de CCIU.
- Un total de 7 cortafuegos de gama baja. Uno para cada una de las seis sedes de menor tamaño, dependientes de las DDTT (sedes con menos de 20 usuarios) y otro para la Oficina de CCIU en el Parlamento Andaluz.
- Una plataforma para la administración centralizada de todos los cortafuegos y el resto de dispositivos que conformarán la nueva APP.
- Una herramienta centralizada de gestión y análisis de los logs generados por los cortafuegos.
- Un firewall a nivel de aplicación (en adelante WAF) para proteger los servidores web alojados en el CPD de CCIU.

5 Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 4 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Lote II: Conmutadores de red y dispositivos de conexión.

- Un core de electrónica de red formado por dos conmutadores o switches de alto rendimiento para la óptima instalación de los nuevos dispositivos que se alojarán en el CPD de CCIU.

4. Consideraciones previas de carácter general.

4.1. Etiquetado de los dispositivos.

Todos los bienes suministrados mediante el presente expediente serán etiquetados para su inventariado por parte de la Junta de Andalucía, de cara a cumplir con lo dispuesto en la Ley 4/86, de 5 de mayo, del Patrimonio de la Comunidad Autónoma de Andalucía en su artículo 14, así como la Orden de 19 de abril de 2006 de desarrollo del Decreto 104/92 de 9 de junio sobre coordinación de la elaboración y desarrollo de la política informática de la Junta de Andalucía.

El etiquetado se realizará mediante etiquetas con tecnología de radiofrecuencia (RFID) que proporcionará la Junta de Andalucía; no obstante, hay que destacar que el proceso completo de etiquetado deberá realizarlo la empresa suministradora, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación.

La empresa contratista deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes que se recoge en el **Anexo IV**, y adoptará todas las medidas necesarias para garantizar que los bienes son entregados con la correspondiente entrada en el Censo de Recursos Informáticos de la Junta de Andalucía (CRIJA) y con la correspondiente etiqueta en los términos que describe el citado procedimiento de inventariado.

4.2. Documentación a entregar.

Con independencia de la documentación que se solicite en otras partes del presente expediente, la empresa adjudicataria deberá facilitar a CCIU la siguiente documentación:

1. Inventario de todo el material y equipo suministrado, incluyendo: marcas, modelos, versiones, números de serie, características y descripción de cada equipo y sus componentes.

2. Relación de las licencias de uso y claves de activación de todas las funcionalidades contratadas, esté el software instalado en los equipos o almacenado en los repositorios del fabricante dispuesto para su descarga.

3. Hojas del producto y/o especificaciones técnicas oficiales del fabricante (*datasheet*) o de terceras empresas de certificación que verifiquen las características de los dispositivos ofertados, manuales de instalación, configuración y uso de todo el equipamiento suministrado.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 5 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

5. Especificaciones técnicas de los dispositivos objeto de esta contratación.

5.1. Observaciones generales relativas a todos los dispositivos.

Dado que las sedes a securizar no cuentan con una infraestructura física adecuada para soportar el despliegue de soluciones virtuales de cortafuegos, y dado que no se prevé que las características de dichas sedes (necesidades de ancho de banda, plantilla, etc) evolucionen en un futuro con la celeridad suficiente para que el factor de la escalabilidad, como ventaja inherente a las soluciones basadas en la virtualización, compensen desde un punto de vista técnico el elevado coste que supondría contemplar esta solución como alternativa, por motivos de eficiencia económica todas las soluciones ofertadas deberán ser dispositivos físicos (*hardware appliances*). Es decir, no se aceptarán soluciones virtuales (*virtual appliances*).

Igualmente, por motivos de seguridad, eficiencia en la utilización del ancho de banda de la RCJA y la dificultad que entrañaría la gestión de las visibilidades de las distintas subredes que conforman actualmente el direccionamiento global de CCIU, tampoco se aceptarán soluciones basadas en la nube (soluciones cloud en cualquiera de sus versiones actuales SaaS, PaaS o IaaS), salvo en el caso de servicios cloud supletorios o complementarios a la solución principal que consuman los propios dispositivos físicos ofertados (por ejemplo un cortafuegos físico que consuma a su vez servicios de sandboxing en la nube, servicio que a priori no está incluido en esta contratación).

Dado el elevado número de sedes a securizar y la escasez de personal técnico dedicado a la gestión de la nueva APP, se ha optado por adquirir una herramienta de gestión centralizada de todos los dispositivos que conformarán dicha Arquitectura, así como una herramienta de análisis a distancia de los logs que dichos dispositivos generen permitiendo de esta forma detectar amenazas de ciberseguridad de forma instantánea. Estas decisiones de diseño de la nueva APP imposibilitan, por motivos de compatibilidad técnica, separar en lotes distintos el conjunto de dispositivos a adquirir, so pena de correr el riesgo de adquirir dispositivos de distintos fabricantes en cada posible lote, haciendo inviable en la práctica la gestión centralizada de toda la APP. Por ello, el Lote I se ha configurado para facilitar que todos los modelos de dispositivos incluidos en dicho Lote puedan ser de la misma marca y del mismo fabricante. No obstante, se podrán ofertar en este Lote dispositivos que siendo de distintos fabricantes o marcas sean totalmente compatibles con la herramienta de gestión centralizada y la herramienta de análisis de logs, siempre que cumplan de forma separada con las especificaciones técnicas de cada tipo de dispositivo recogidas en este PPT.[6]

Por otra parte, no se admitirán modelos de dispositivos que a la fecha de finalización del plazo establecido para la presentación de ofertas, se encuentren descatalogados (*legacy models*) o su fecha de

6 Es preciso destacar que, en la actualidad, la mayoría de fabricantes de reconocido prestigio y amplia presencia en el ámbito de la ciberseguridad cuentan con la totalidad de los dispositivos que se pretenden adquirir en sus catálogos. Por ello, incluir el requisito de procedencia de un mismo fabricante para todos los dispositivos del Lote I por motivos de compatibilidad en estas prescripciones técnicas, no hace referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los productos ofrecidos por un empresario determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados, con la finalidad de favorecer o descartar ciertas empresas de antemano o a ciertos productos.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 6 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

descatalogación facilitada por el fabricante sea conocida públicamente y resulte inferior a la fecha obtenida al sumar el periodo mínimo de garantía (2 años) a la fecha de finalización del citado plazo. Esta prohibición no afectará a aquellos dispositivos de fabricantes que explícitamente adopten como política de marketing la renovación de su catálogo de productos o series de productos con una periodicidad conocida (por ejemplo anual). En estos casos, habrá que estar a las prescripciones recogidas en el apartado que regula la garantía en este mismo pliego. En esta línea, por idénticos motivos, no se admitirán ninguno de los modelos recogidos en el **Anexo I.**

En aquellos casos que se desplieguen dos dispositivos en alta disponibilidad, los dispositivos a instalar serán idénticos, es decir, de la misma marca, modelo, actualización del hardware y versión del sistema operativo con objeto de configurarlos en modo activo/activo o activo/pasivo según convenga.

En general, para todos los dispositivos incluidos en esta contratación, y en cuanto a las dimensiones requeridas se refiere, por motivos de economía de espacio tanto en el CPD de CCIU como en los centros de datos o salas técnicas de las distintas sedes, todos los modelos de dispositivos ofertados deberán poder montarse en racks de 19" de anchura, con 1 o 2 U de altura como máximo. En aquellos casos en los que los modelos ofertados sean del tipo escritorio (*desktop*), la empresa contratista deberá incluir en su oferta el correspondiente "kit de montaje en rack" para posibilitar dicho montaje. El accesorio deberá ser el oficial propio del modelo de dispositivo ofertado facilitado por el fabricante. Solo en caso de no comercializarse éste, se podrá ofertar otro distinto, pero en cualquier caso, el accesorio ofertado deberá permitir llevar todas las conexiones principales (incluido el puerto consola) del dispositivo a la parte frontal del rack si en su diseño original se dispusiesen en la parte posterior del mismo.

5.2. Especificaciones técnicas de los cortafuegos (incluidos en el LOTE I).

5.2.1. Consideraciones previas relativas a los cortafuegos.

Grosso modo, por las prestaciones exigidas, serán cortafuegos de nueva generación, conocidos en el argot habitual en ciberseguridad como firewalls NGFW o UTM (ver Anexo III: Glosario de términos, acrónimos y abreviaturas) según los modelos y rendimiento esperado. En concreto, serán dispositivos que además del funcionamiento convencional de los firewalls o cortafuegos tradicionales deberán incluir al menos las siguientes funcionalidades:[7]

A) Sin necesidad de contratar periódicamente licencias de uso del software:

A.1) Compatibles con el nuevo estándar de direccionamiento IPv6.

A.2) Capacidad de funcionar en modo router/NAT o en modo transparente.

A.3) Capacidad de enrutamiento: tanto estático como dinámico, y la capacidad de establecer

7 Por funcionalidades tradicionales de los firewalls entendemos en este contexto el control de tráfico de red inspeccionando la cabecera de los paquetes o tramas hasta el nivel 4 del modelo OSI.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 7 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

políticas avanzadas de enrutamiento (*policy routing*).[8]

A.4) Capacidad de trabajar con dominios virtuales (VDOM).

A.5) Configuración como servidor proxy (HTTP, FTP).

A.6) Configuración en alta disponibilidad (activo/activo, activo/pasivo).

A.7) Posibilidad de configurar políticas basadas en la calidad del servicio (QoS). Incluyendo gestión de ancho de banda (*traffic shaping*) tanto por políticas como por IP o interfaces.

A.8) Soporte para establecimiento de VPN (tanto IPsec-VPN como SSL-VPN).[9]

A.9) Capacidad de inspección del contenido SSL, al menos en los protocolos más comunes (HTTPS, SMTPS, POP3S, FTPS e IMAPS).

A.10) Capacidad de inspección del contenido en túneles SSH.

A.11) Identificación de dispositivos. Permitir identificar el tipo de dispositivo que se conecta a la red. Para obtener visibilidad de inmediato de usuarios, sistema operativo, dirección IP, la MAC, etc.

B) Susceptibles de ser contratadas bajo un régimen de licenciamiento periódico:

B.1) Protección antimalware avanzada: protección antivirus y otros malwares comunes (tanto por escaneo de firmas como por análisis heurístico), permitiendo incluso el bloqueo de ficheros.

B.2) Sistema de detección/prevención de intrusiones (IDS/IPS) en tiempo real. El motor IDS deberá proveer seguridad hasta la capa de aplicación (*multilayer IDS/IPS*). El IPS deberá detectar y prevenir al menos los siguientes tipos de ataques:

B.2.1) Ataques de Denegación de Servicio (DoS).[10]

B.2.2) Ataques de reconocimiento del sistema.[11]

B.2.3) Exploits del tipo *Brute Force attack, CGI Scripts, Web Server attacks, Web Browser attacks, SMTP attack, IMAP/POP attack, Buffer overflow, DNS attacks, IP spoofing* y la familia de *Trojan Horse attacks.*

B.2.4) Ataques de evasión de sondas IDS. Como mínimo detectará las siguientes técnicas de evasión: *signature spoofing, signature encoding, IP fragmentation, TCP/UDP disassembly* y *obfuscation*.

B.2.5) Botnets.

B.3) Filtrado de tráfico web (*URL Web Filtering*). Mediante el uso de listas blancas/negras de

8 Políticas de enrutamiento basadas en otros parámetros además de la red de destino como la interfaz de origen o la red de origen, el protocolo, servicio o rango de puertos tanto de origen como de destino etc.

9 Aunque en la actualidad este servicio está soportado por la RCJA se considera adecuado incluirlo entre los requisitos de los cortafuegos a adquirir por razones de oportunidad.

10 El IPS detectará al menos los siguientes ataques de DoS más comunes: inundación de paquetes, incluyendo Smurf flood, TCP SYN flood, UDP flood, y ICMP flood; así como paquetes formados incorrectamente, incluyendo Ping of Death, Chargen, Tear drop, land, y WinNuke.

11 La funcionalidad IPS detectará al menos los siguientes ataques de reconocimiento más comunes: Fingerprinting, Ping sweeps, Port scans (tanto TCP como UDP), Buffer overflows (incluyendo SMTP, FTP y POP3), Account scans y OS identification (Identificación del Sistema Operativo)

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 8 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

URL, mediante listas locales de contenido, filtrado de scripts de código malicioso del tipo java applets, cookies y ActiveX, y filtrado de contenido en cachés de los motores de búsqueda.

B.4) Control a nivel de aplicación (nivel 7 del modelo OSI). Detectar y tomar medidas contra el tráfico de red en función de la aplicación, incluso si el tráfico utiliza los puertos o protocolos no estándar.

B.5) Prevención de fuga de datos (*Data Leak Prevention*). Para transferencia de mensajes deberá inspeccionar al menos los servicios SMTP, POP3, IMAP, HTTP, NNTP e IMAP. A su vez, para transferencia de ficheros añadirá a los servicios anteriores, al menos los de FTP, AIM, ICQ, MSN, Yahoo! y MAPI.

Todos los modelos de cortafuegos ofertados deberán poder gestionarse conjuntamente a través de la plataforma de administración o gestión centralizada incluida en esta contratación.

Del mismo modo, todos los modelos deberán ser compatibles con la herramienta de gestión de logs que también se incluye en esta contratación. Es decir, todos los cortafuegos deberán ser capaces de enviar sus logs periódicamente a la herramienta de gestión centralizada de logs facilitándoles la dirección ip de esta última. Esta transmisión de logs será directa dispositivo a dispositivo (no se aceptarán soluciones cloud intermedias) y podrá ser encriptada si así se requiriese.

Asimismo, para todos los cortafuegos ofertados, la empresa contratista deberá incluir en su oferta las licencias anuales de actualización y uso del software del paquete de funcionalidades citadas en el apartado B), bien de forma individual o agrupadas según la estrategia de marketing de cada fabricante. En concreto, por su naturaleza, se entiende a priori que estas licencias posibilitarán, en cualquier caso e ineludiblemente, las actualizaciones periódicas del software correspondiente a las funcionalidades siguientes:

B.1) Protección antimalware avanzada.

B.2) Sistema de detección/prevención de intrusiones (IDS/IPS).

B.4) Control a nivel de aplicación.

B.5) Prevención de fuga de datos (*Data Leak Prevention*).

No se está interesado en la actualización periódica de listados de sitios web o urls prohibidos o no recomendables, por lo que la funcionalidad de filtrado dinámico de sitios web (la funcionalidad B.3) no se incluirá necesariamente entre las licencias ofertadas (aunque todos los cortafuegos deberán incluir la posibilidad de configurarlos manualmente con este objetivo si así se requiriese), por asumirla directamente RCJA en la actualidad.

Respecto al rendimiento de los cortafuegos, de forma general y para facilitar las comparativas entre los modelos de distintos fabricantes, se han distinguido cuatro niveles de pruebas de carga o estrés, según la naturaleza del tráfico inspeccionado y el número de servicios o nuevas funcionalidades que se mantengan activadas:

- **Nivel I**: nivel de estrés bajo. Se monitoriza el rendimiento del firewall en el procesamiento de

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 9 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

paquetes UDP sin analizar su interior (*raw packet processing performance*). El objetivo de esta prueba es determinar la capacidad de procesamiento de paquetes en bruto de cada par de puertos en línea del firewall, así como su eficacia para reenviar paquetes rápidamente a fin de proporcionar el nivel de rendimiento más alto de la red y su nivel de latencia más bajo. Se utiliza direccionamiento IPv4 y tráfico de paquetes UDP de 1518/512/64 bytes.[12]

- **Nivel II**: nivel de estrés medio, incorporando a las prestaciones básicas del nivel anterior el servicio IPS simulando un tráfico real en un entorno empresarial según el estándar *Enterprise Traffic Mix* y con el sistema de logs activado.[13]
- **Nivel III**: nivel de estrés alto, se supondrá medido con las funcionalidades del Nivel II activadas, e incluirá además el control a nivel de aplicación, en todo caso con el sistema de logs también activado.
- **Nivel IV**: nivel de estrés muy alto, se supondrá medido con las funcionalidades del Nivel III activadas, e incluirá además el servicio de protección antimalware avanzado, activando en las mismas condiciones que el nivel anterior el sistema de logs.

Siguiendo con cuestiones relativas al rendimiento exigido, dada la diversidad de sedes a securizar y sus distintas necesidades y previsiones de crecimiento, se ha optado por clasificar los cortafuegos a adquirir en cuatro categorías, conformando la siguiente tipología:

- **Modelo XL**: destinado a securizar el CPD de CCIU alojado actualmente en el edificio del ZOCO en el municipio de Tomares.
- **Modelo L**: destinado a securizar las sedes principales de las DDTT y la sede de los SSCC de CCIU en el edificio Kepler en la Isla de la Cartuja.
- **Modelo M**: destinado a securizar las sedes secundarias de las DDTT de mayor tamaño y previsión de crecimiento (sedes por lo general con menos de 80 y más de 20 usuarios).
- **Modelo S**: destinado a securizar las restantes sedes con acceso a Internet de las DDTT (sedes con menos de 20 usuarios y escasa o nula previsión de crecimiento) y la Oficina de CCIU en el Parlamento Andaluz.

Las empresas licitadoras podrán incluir en sus ofertas cualquier conjunto de cortafuegos de cualquier marca o fabricante siempre que las características técnicas, y las prestaciones reales del dispositivo sean iguales o superiores a las establecidas en el presente pliego en todas y cada una de las categorías de cortafuegos establecidas, con la condición ineludible ya citada de que todos los dispositivos incluidos en el **Lote I** deben ser del mismo fabricante o compatibles con la herramienta de gestión centralizada y la herramienta de análisis de logs.

A continuación, se detallan las especificaciones técnicas de cada modelo tipo en cada una de las

12 Máximo número de tramas por segundo por 1 Gigabit de tráfico: 81.000/234.000/1.488.000.
13 Enterprise Traffic Mix: en resumen se trata de un tráfico compuesto de un 30% de tráfico HTTP y un 70% de tráfico HTTPS de una combinación de aplicaciones y sitios web como Facebook, WhatsApp, Dropbox, Office 365, etc.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 10 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

categorías. En aras de facilitar la lectura del documento esta información se ha resumido en el **Cuadro 1** del **Anexo II**.

Las especificaciones técnicas de los modelos ofertados deberán ser acreditadas con la documentación oficial del fabricante, si bien los datos relativos al rendimiento podrán ser acreditados a partir de los resultados obtenidos por una tercera empresa de certificación (independiente del fabricante y de reconocido prestigio a nivel internacional en el ámbito de la ciberseguridad). Tanto la documentación técnica del fabricante, como los informes de rendimientos o *reviews* técnicas realizadas por terceras empresas se incluirán en la documentación que acompañará a la oferta con cada modelo, so pena de quedar eliminada del proceso de licitación.

5.2.2. Especificaciones técnicas del modelo XL.

Los dos cortafuegos de esta categoría se destinarán a securizar el tráfico del CPD de CCIU, configurados en alta disponibilidad (activo/activo o activo/pasivo según convenga).

En concreto, se pretende adquirir un modelo de cortafuegos de gama media-alta que al funcionamiento propio de los cortafuegos tradicionales incorpore las funcionalidades de los dispositivos de nueva generación ya descritas, con las siguientes características principales de rendimiento como mínimo según los niveles de estrés definidos:

- Nivel I: 36/36/22 Gbps
- Nivel II: 5,2 Gbps
- Nivel III: 5 Gbps
- Nivel IV: 4,5 Gbps

La oferta del modelo correspondiente a esta categoría deberá incluir de forma separada las licencias de uso y actualización del software que permita el funcionamiento óptimo de las funcionalidades relacionadas en el **apdo. 5.2.1 durante un año**.

Asimismo, el modelo de cortafuegos ofertado en esta categoría deberá permitir crear un perfil de seguridad enfocado a la protección contra amenazas de aplicaciones web. El sistema incluirá una lista de firmas y ataques reconocidos (por ejemplo del tipo *cross site scripting*, *sql injection*, etc.) que se puedan aplicar a políticas de seguridad, o permitir la opción de redirigir el tráfico web al dispositivo WAF incluido en la solución global, para proceder a su análisis.

La empresa licitadora incluirá obligatoriamente en su oferta un total de **4** transceptores de fibra óptica de alta velocidad 10GE SFP+ (10GBase-SR) para conectores LC Duplex compatibles con el modelo de cortafuegos ofertado para su conexión en alta disponibilidad con el core de conmutadores.

El detalle de las especificaciones técnicas mínimas exigidas para este modelo se resumen en el **Cuadro 1** del **Anexo II**.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 11 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

5.2.3. Especificaciones técnicas del modelo L.

Los cortafuegos de esta categoría, configurados en alta disponibilidad (activo/activo o activo/pasivo según convenga), se destinarán a securizar las instalaciones de los SSCC de CCIU en el edificio Kepler y las ocho sedes principales de las DDTT.

En detalle, en este caso se pretende adquirir un tipo de cortafuegos de gama media que al funcionamiento propio de los cortafuegos tradicionales incorpore las funcionalidades de los cortafuegos de nueva generación ya descritas, con las siguientes características principales de rendimiento (como mínimo) según los niveles de estrés definidos:

- Nivel I: 7,4/7,4/4,4 Gbps
- Nivel II: 500 Mbps
- Nivel III: 350 Mbps
- Nivel IV: 250 Mbps

La oferta del modelo correspondiente a esta categoría deberá incluir de forma separada las licencias de uso y actualización del software que permita el funcionamiento óptimo de las funcionalidades relacionadas en el **apdo. 5.2.1** durante un año.

El detalle de las especificaciones técnicas mínimas exigidas para este modelo se recogen en el **Cuadro 1**.

5.2.4. Especificaciones técnicas del modelo M.

Los cortafuegos de esta categoría, configurados en alta disponibilidad (activo/activo o activo/pasivo según convenga), se destinarán a securizar las sedes secundarias de las DDTT (sedes con un número de usuarios entre 20 y 80 y un ancho de banda actual menor de 100 Mbps pero con cierta tendencia a aumentar en algunos casos) y el laboratorio de ciberseguridad de CCIU.

En definitiva, se pretende adquirir un modelo de cortafuegos de gama media-baja que a las funcionalidades propias de los cortafuegos tradicionales incorpore las funcionalidades de los cortafuegos de nueva generación ya descritas, con las siguientes características de rendimiento principales como mínimo según se activen un mayor número de servicios:

- Nivel I: 4/4/4 Gbps
- Nivel II: 450 Mbps
- Nivel III: 350 Mbps
- Nivel IV: 250 Mbps.

La oferta del modelo correspondiente a esta categoría deberá incluir de forma separada las licencias de uso y actualización del software que permita el funcionamiento óptimo de las funcionalidades relacionadas

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 12 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

en el **apdo. 5.2.1** durante un año.

El detalle de las especificaciones técnicas mínimas exigidas se recogen en el **Cuadro 1**.

5.2.5. Especificaciones técnicas del modelo S.

Los cortafuegos de esta categoría no se configurarán en principio en alta disponibilidad, pero los dispositivos ofertados deberán permitir dicha configuración por razones de escalabilidad en un futuro. Se destinarán a securizar las sedes de menor tamaño de las DDTT (sedes con un número actual de usuarios menor de 20 y un ancho de banda menor de 50 Mbps y con escasa o nula previsión de crecimiento).

En concreto, se pretende adquirir un modelo de cortafuegos de gama baja que a las funcionalidades propias de los cortafuegos tradicionales incorpore las prestaciones de los cortafuegos de nueva generación ya descritas, con las siguientes características de rendimiento principales como mínimo según se activen un mayor número de servicios:

- Nivel I: 3/3/3 Gbps
- Nivel II: 400 Mbps
- Nivel III: 250 Mbps
- Nivel IV: 200 Mbps.

La oferta del modelo correspondiente a esta categoría deberá incluir de forma separada las licencias de uso y actualización del software que permita el funcionamiento óptimo de las funcionalidades relacionadas en el **apdo. 5.2.1** durante un año.

El detalle de las especificaciones técnicas mínimas exigidas para este modelo se recogen en el **Cuadro 1**.

5.3. Especificaciones técnicas de la plataforma de gestión centralizada (incluida en el LOTE I).

Con objeto de disminuir los costes de despliegue de las actualizaciones de software y el resto de operaciones de mantenimiento de toda la APP, la plataforma de gestión centralizada deberá incluir las siguientes funcionalidades:

1. Control y seguimiento de configuraciones. La herramienta guardará y mantendrá el historial de todos los cambios de configuración que se hagan a lo largo del tiempo. Estos cambios se podrán programar para aplicarlos de forma automática.

2. Gestión centralizada. La herramienta podrá gestionar de forma centralizada la configuración de múltiples equipos desde una misma consola. Las configuraciones se podrán compilar en un repositorio centralizado y desplegar en múltiples dispositivos cuando sea requerido.

3. Dominios de administración. La herramienta podrá dividir la administración de grandes entornos

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 13 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

agrupando equipos en dominios de administración a nivel de sede, delegación territorial, etc.

4. Provisión local del servicio de actualizaciones de software de los cortafuegos. Un cortafuegos podrá utilizar la plataforma para optimizar el rendimiento en la búsqueda de clasificaciones y la descarga de definiciones y firmas para antivirus, IPS, etc.

5. Gestión de firmwares. La herramienta podrá gestionar de forma centralizada imágenes de firmware y programar la actualización de los dispositivos gestionados.

6. Informes y logging. La herramienta se integrará completamente con la herramienta de gestión de logs incluida en la oferta (**apdo. 5.4**) para permitir el descubrimiento, análisis, priorización e informes de los eventos de seguridad de la red.

7. Gestión del ciclo de vida de los dispositivos que conforman la APP: despliegue, monitorización, mantenimiento y actualización.

8. Capacidad de gestionar de forma centralizada un mínimo de 100 dispositivos.

9. Compatibilidad con el nuevo direccionamiento IPv6.

La oferta deberá incluir de forma separada la licencia anual pertinente para realizar las actualizaciones del firmware y del software que se produzcan durante dicho periodo.

Asimismo, la oferta incluirá obligatoriamente 2 transceptores de fibra óptica 1GE SFP para conectores LC Duplex, compatibles con el dispositivo, con objeto de conectarlo en alta disponibilidad con el core de conmutadores mediante cableado de fibra óptica 850 nm multimodo. Siempre que el dispositivo dispusiese de una interfaz con esta características, de lo contrario, se conectará con cableado de cobre compatible con 1GE RJ45.

El detalle de las especificaciones técnicas del hardware mínimas exigidas para este dispositivo se recogen en el **Cuadro 2.**

5.4. Especificaciones técnicas de la herramienta de gestión de logs (incluida en el LOTE I).

Se pretende adquirir una herramienta para la gestión centralizada de los logs de los dispositivos que conforman la APP, la herramienta permitirá el análisis de los mismos y la creación de informes. Las funcionalidades mínimas exigidas se detallan a continuación:

1. Generar informes periódicos y de forma automatizada, fácilmente configurables, para ayudar a monitorizar y mantener identificados patrones de ataques, políticas de uso aceptable o en su caso demostrar el cumplimiento o incumplimiento de las políticas establecidas.

1.1. Informes de ataques: ataques registrados por cada dispositivo de seguridad, señalando el momento en el que son registrados, e identificados a las fuentes más comunes de ataque

1.2. Informes de virus: top virus detectados, virus detectados por protocolo, etc.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 14 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

1.3. Informe de eventos: eventos propios de cada máquina, de administración de la misma, etc.

2. Generar informes sobre la capacidad y utilización de las subredes, que permitan gestionarlas de una forma más eficiente.

2.1. Informe de utilización del tráfico web: usuarios web top, sitios bloqueados, usuarios de mayor frecuencia de intento de acceso a sitios bloqueados, etc.

2.2. Informe de utilización de ancho de banda: informes de uso del ancho de banda por usuario, día, hora y protocolo

2.3. Informes por protocolo: protocolos más utilizados, usuarios ftp /telnet etc..

3. Funcionalidades avanzadas, tales como la correlación de eventos, análisis forense y vulnerabilidades de los activos o scanning de red.

4. Agregación segura de datos desde múltiples dispositivos de seguridad, para proporcionar una visibilidad completa de la APP.

5. Integración completa con la herramienta de gestión centralizada (**apdo. 5.3**).

6. Segmentación de la información generada por los distintos cortafuegos en dominios administrativos permitiendo modelos de delegación basados en roles. De forma que se pueda gestionar independientemente la información generada por sede, delegación territorial, etc.

7. Ciclo completo de gestión de la información que abarca los procesos de recolección, normalización, clasificación, correlación de eventos y explotación en modo de alertas e informes.

8. Compatible con el nuevo direccionamiento IPv6.

9. Capacidad de tratar los logs generados por cualquier dispositivo que sea compatible con Syslog.

10. Ejecución de diferentes utilidades de diagnóstico, tales como: ping, traceroute y visor de logs.

11. Servicios de integración web desde terceras aplicaciones vía servicios web.

12. Posibilidad de realizar backups/restore de logs e informes.

13. La herramienta permitirá su gestión a través de un interfaz gráfico basado en Web (GUI) bajo el protocolo HTTPS, por razones de seguridad (una consola web de gestión). Esta interfaz será compatible con las últimas versiones de los principales navegadores web del mercado (Microsoft Internet Explorer, Mozilla Firefox y Google Chrome) en la fecha que finalice el plazo de presentación de ofertas.

14. Posibilidad de sincronización horaria con servidores NTP externos configurable por el administrador de la herramienta.

15. La solución ofertada contará con una herramienta gráfica que simplifique la creación de nuevas

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 15 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

consultas a la base de datos.

La oferta deberá incluir de forma separada la licencia anual pertinente para realizar las actualizaciones del firmware y del software que se produzcan durante dicho periodo.

Asimismo, la oferta incluirá obligatoriamente 2 transceptores de fibra óptica 1GE SFP para conectores LC Duplex, compatibles con el dispositivo, con objeto de conectarlo en alta disponibilidad con el core de conmutadores mediante fibra óptica 850 nm multimodo. Si el dispositivo dispusiese de una interfaz con esta características, de lo contrario, se conectará con cableado de cobre compatible con 1GE RJ45.

El detalle de las especificaciones técnicas del hardware mínimas exigidas para este dispositivo se recogen en el **Cuadro 3**.

5.5. Especificaciones técnicas del firewall a nivel de aplicación (WAF) (incluido en el LOTE I).

Con objeto de proporcionar una protección completa y especializada a todos los niveles para las aplicaciones y servicios web de CCIU, se pretende adquirir un cortafuegos o firewall a nivel de aplicación (WAF) de gama media (modalidad *hardware appliance*). Esta capa de seguridad permitirá disminuir el riesgo de ataques especialmente contra el elenco de aplicaciones web desplegadas en la actualidad en los entornos de producción de CCIU que por su antigüedad y escaso uso no se actualizan con la periodicidad deseable.

Asimismo, estos dispositivos cuenta con la posibilidad de balancear el tráfico HTTP/HTTPS si las aplicaciones web a proteger se encuentran desplegadas en un cluster de servidores web. Esto permitirá en un futuro configurar un despliegue que mejore la ralentización actual de algunos de nuestras aplicaciones web.

El modelo a ofertar se ajustará a las siguientes características y funcionalidades mínimas:

1. Respecto a las opciones de despliegue, deberá permitir su despliegue en las siguientes alternativas:

   1.1. Modo "inspección transparente": en forma de "bridge" de nivel dos, o sea sin producir ningún impacto a nivel de routing ni cambio en la topología lógica de la red.

   1.2. Modo "*reverse proxy*": configurando el WAF a nivel tres, para permitir funcionalidades como *URL rewrite*, balanceo o *SSL offloading*.

   1.3. Modo "*offline sniffing*": analizando el tráfico de datos en una ruta paralela sin producir ningún impacto en la red ni el los servicios auditados.

2. En cuanto a su funcionamiento, deberá seguir un "modelo de seguridad positiva" creando un perfil de seguridad inteligente adaptado a cada aplicación que protega a éstas de cualquier vulnerabilidad conocida o desconocida como ataques "*zero-day*", *sql-injection*, *cross-site scripting* o cualquier otro ataque a nivel de aplicación.

3. Gestión de la autenticación: la herramienta permitirá descargar a los servidores web de las tareas de autenticación, soportando, al menos, los siguientes tipos de autenticación: local, autenticación

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 16 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

contra servidores LDAP o RADIUS con opción de doble factor de autenticación, RSA SecurID y SSO.

4. Despliegue en alta disponibilidad: en modo activo-activo o activo-pasivo, proporcionando sincronización automática de las configuraciones entre ambos nodos.[14]

5. Administración delegada de la herramienta (o al menos de algunas de sus funcionalidades) según distintos "dominios administrativos".

6. Balanceo de carga: capacidad de repartir las conexiones que se dirijan a distintos servidores configurados en granjas. La herramienta soportará al menos los siguientes algoritmos de balanceo:

6.1. *Round Robin*.

6.2. *Weighted Round Robin*.

6.3. *Least Connection*.

7. Gestión del tráfico HTTPS: en cuanto a la gestión del tráfico encriptado vía SSL, la herramienta deberá permitir tanto terminar el túnel SSL en ella (*SSL offloading*), como inspeccionar el tráfico encriptado destinado a un servidor (*SSL inspection*), cargando los certificados con su clave pública y privada sin necesidad de terminar el túnel SSL en la propia herramienta.

8. Prevención de ataques de tipo DoS: la herramienta contará con la capacidad de detectar e impedir ataques de denegación de servicio tanto en las capas 3 y 4 como en la capa 7 del modelo OSI (*Layer 7 Denial of Service*)

9. Prevención de ataques desconocidos o "*zero day attacks*".

10. Generación de logs/informes: la herramienta contará con la capacidad de proporcionar informes tanto predefinidos como creados de forma personalizada para analizar los distintos ataques, eventos y los flujos de tráfico. Deberá ser compatible con la herramienta de gestión de logs incluida en esta oferta (**apdo. 5.4**).

11. Protección a nivel de aplicación: la herramienta contará con un diccionario de firmas de ataques actualizado periódicamente y con un motor de escaneo que se ocupe de escanear el tráfico entrante y saliente, identificando cada elemento que se corresponda con un "exploit" conocido y predefinido. Este motor de escaneo deberá permitir a CCIU desarrollar sus propias firmas mediante el uso de expresiones regulares, con objeto de crear firmas nuevas y completamente personalizadas para cada aplicación y vulnerabilidad.

12. Prevención de fuga de datos (DLP, *Data Leak Prevention*): la herramienta permitirá proteger frente a robos de información contenida en las aplicaciones monitorizando cuidadosamente todo el tráfico saliente. Deberá permitir a CCIU crear sus propias firmas y patrones de DLP de forma totalmente

14 Aunque solo se pretende adquirir un dispositivo, está característica es necesaria por motivos de escalabilidad de la APP en un futuro.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 17 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

granular, combinándolas con las reglas predefinidas para lograr una protección completa contra todo tipo de ataques y eventos.

13. Cumplimiento de los estándares RFC para el protocolo HTTP: la herramienta será capaz de bloquear cualquier ataque que trate de manipular el protocolo HTTP asegurando el cumplimiento estricto de los estándares RFC con la finalidad de proteger frente a ataques como "*enconding attacks*", "*buffer overflow*" y cualquier otro ataque específico de aplicación.

14. Políticas de acceso a web: la herramienta asegurará el correcto acceso a las aplicaciones web siguiendo la lógica del negocio para evitar ataques de "*Cross Site Request Forgery* (CSRF)". Incluyendo la posibilidad de configurar políticas de página web de inicio (*Start Pages policy*).

15. Análisis de vulnerabilidades: la herramienta deberá contar con un módulo de escaneo de vulnerabilidades actualizado periódicamente capaz de escanear y analizar de forma automática las aplicaciones web, detectando las debilidades y vulnerabilidades conocidas y desconocidas de las mismas (al menos las relacionadas en el OWASP Top 10). Además deberá permitir su integración con escáneres de terceros. Pudiendo mediante la importación de reportes de terceros generar firmas para proteger las vulnerabilidades descubiertas por estos.

16. Compatible con el direccionamiento IPv6.

17. Compatible con la plataforma de administración centralizada incluida en este pliego (**apdo. 5.3**).

La oferta deberá incluir de forma separada la licencia anual pertinente para realizar las actualizaciones del firmware y del software que se produzcan durante dicho periodo. No se admitirán licencias basadas en número de usuarios o servidores web a proteger.

Asimismo, la oferta incluirá obligatoriamente 2 transceptores de fibra óptica 10GE SFP+ (10GBase-SR) para conectores LC Duplex, compatibles con el dispositivo, con objeto de conectarlo en alta disponibilidad con el core de conmutadores mediante fibra óptica de alta velocidad.

El detalle de las especificaciones técnicas del hardware mínimas exigidas para este tipo de dispositivo se recogen en el **Cuadro 4**.

5.6. Especificaciones técnicas de los switches o conmutadores de red (incluidos en el LOTE II).

Se pretende adquirir 2 switches o conmutadores de red de alto rendimiento idénticos para ampliar el actual core de comunicaciones del CPD de CCIU de reciente adquisición.[15] Por ello, la solución ofertada deberá, como condición ineludible, poder conectarse en alta disponibilidad a través de cableado de fibra óptica 10G SFP+ con los dos switches actuales (ver **apdo. 5.7**).

15 Actualmente se dispone de dos switches Huawei S6720-54C-EI-48S-AC configurados en stacking a 40G QSFP+.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 18 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

En concreto, se pretende adquirir dos switches con las siguientes características o especificaciones técnicas mínimas:

1. Formato compacto (altura de 1U).
2. Doble fuente de alimentación intercambiable en caliente.
3. Al menos 24 slots 10G SFP+, compatibles con 1GB SFP.
4. Al menos 2 puertos 40G QSFP+ (para realizar stacking entre ellos).
5. Capacidad de transmisión: 2,56 Tbps.
6. Rendimiento de reenvío de paquetes: 720 Mpps.
7. Latencia promedio máxima: 1 µs.
8. Al menos 1 puerto serie y 1 puerto USB.
9. Posibilidad de configuración mediante línea de comandos (SSH) y mediante interfaz web (HTTPS).

Además deberán contar con soporte para, como mínimo, los siguientes protocolos:

- Enrutamiento IPv4:
  - Enrutamiento estático, RIPv1, RIPv2, ECMP y URPF
  - OSPF, IS-IS y BGP
  - VRRP
  - Enrutamiento basado en políticas
- Enrutamiento IPv6
  - Ruta estática
  - RIPng
  - OSPFv3
  - BGP4+
  - ISISv6
- Multidifusión
  - Dirección MAC multidifusión de capa 2 estática
  - Reenvío de multidifusión en función de la MAC
  - Snooping y fast leave de IGMP
  - VLAN multidifusión
  - Snooping de MLD
  - Proxy de IGMP

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 19 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- Multidifusión controlable
- Estadísticas de tráfico multidifusión en función del puerto
- IGMP v1/v2/v3
- PIM-SM, PIM-DM, and PIM-SSM
- MSDP
- MVPN

En cuanto a las herramientas para asegurar un determinado nivel o calidad del servicio en el redireccionamiento del tráfico, deberá contar con las siguientes funcionalidades:

- Limitación de velocidad de los paquetes enviados y recibidos por una interfaz
- Redireccionamiento de paquetes
- Control de tráfico en función del puerto y CAR de dos velocidades y tres colores
- Ocho colas en cada puerto
- Algoritmos de planificación de colas WRR, DRR, SP, WRR+SP y DRR+SP
- Remarcado de prioridades 802.1p y DSCP
- Filtrado de paquetes en las capas 2 a 4; filtrado de tramas no válidas según la dirección MAC de origen, la dirección MAC de destino, la dirección IP de origen, la dirección IP de destino, el número de puerto, el tipo de protocolo y la ID de VLAN
- Limitación de la velocidad en cada cola y conformación de tráfico en puertos

Por último, las características que deben poseer en el ámbito de la seguridad son las siguientes:

- Administración de privilegios de usuarios y protección mediante contraseñas
- Protección contra ataques DoS, ARP e ICMP
- Vinculación de dirección IP, dirección MAC, interfaz y red VLAN
- Aislamiento de puertos, seguridad de puertos y direcciones MAC fijas
- Entradas de direcciones MAC blackhole
- Restricción de la cantidad de direcciones MAC aprendidas
- Autenticación 802.1x y restricción de la cantidad de usuarios en una interfaz
- Autenticación AAA, RADIUS y TACACS
- SSH v2.0
- Protocolo seguro de transferencia de hipertexto (HTTPS)
- Protección de la CPU
- Lista negra y lista blanca

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 20 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Un resumen de las especificaciones técnicas principales de estos conmutadores se recoge en el **Cuadro 5**.

Por otra parte, la oferta incluirá también:

- Un par de cables de conexión de alta velocidad QSFP+ 40G, con una longitud mínima de 0,5 m, homologados por el fabricante de los conmutadores para realizar el apilamiento físico (*stacking*) entre ellos.

5.7. Especificaciones técnicas de los transceptores y el cableado de conexión (incluidos en el LOTE II).

Para facilitar a las empresas contratistas la redacción de sus ofertas, se ha recogido en este apartado el número y las características de los transceptores compatibles con el core de conmutadores que obligatoriamente deberán incluir en sus ofertas del **Lote 2**. En este **Lote 2** se ha incluido también el cableado necesario para la instalación de todos los dispositivos en un rack.

1) Conexión en alta disponibilidad del core actual (2 switches Huawei S6720-54C-EI-48S-AC) con el nuevo core (2 switches ofertados). Esta conexión se realizará utilizando cableado de fibra óptica de 10Gigabit-SFP+, de forma que cada conmutador de un core se conecte con los dos conmutadores del otro core.

- **4** transceptores de fibra óptica multimodo 10Gigabit-SFP+ (850nm, conector LC-Duplex).
- Cableado: **4** cables o latiguillos de fibra óptica (multimodo, de banda ancha OM3, núcleo de fibra de 50/125µm, 10Gigabit-SFP+, 850nm), conectores LC Duplex- LC Duplex, de **10** metros.

A modo de orientación los transceptores de 10G SFP+ utilizados en la actualidad en los switches Huawei responden a las siguientes características:

- Transceiver Type: 10GBASE_USR_SFP
- Connector Type: LC
- Wavelength (nm): 850
- Transfer Distance (m): 50 (50um), 20 (62.5um), 100 (OM3)
- Digital Diagnostic Monitoring: YES
- Vendor Name: HUAWEI

2) Conexión en alta disponibilidad nuevo core (2 switches ofertados) con los 2 cortafuegos modelo XL (en el mismo rack). Esta conexión se realizará obligatoriamente utilizando conexiones de fibra óptica de 10Gigabit-SFP+, de forma que cada uno de los dos cortafuegos modelo XL se conecte con los dos conmutadores del nuevo core.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 21 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- **4** transceptores de fibra óptica multimodo 10Gigabit-SFP+ (850nm, conector LC Duplex) (10GEBase-SR).
- Cableado: **4** cables o latiguillos de fibra óptica (multimodo, de banda ancha OM3, núcleo de fibra de 50/125µm, 10Gigabit-SFP+, 850nm), conectores LC Duplex- LC Duplex, de **1** metro.

3) Conexión en alta disponibilidad nuevo core (2 switches) con el WAF (en el mismo rack). Esta conexión se realizará obligatoriamente utilizando conexiones de fibra óptica de 10Gigabit-SFP+, de forma que el WAF se conecte con los dos conmutadores del nuevo core a través de sus 2 puertos 10Gigabit-SFP+.

- **2** transceptores de fibra óptica multimodo 10Gigabit-SFP+ (850nm, conector LC Duplex) (10GEBase-SR).
- Cableado: **2** cables o latiguillos de fibra óptica (multimodo, de banda ancha OM3, núcleo de fibra de 50/125µm, 10Gigabit-SFP+, 850nm), conectores LC Duplex- LC Duplex, de **1** metro.

4) Conexión nuevo core (2 switches) con la plataforma de administración centralizada (en el mismo rack). Dado que como mínimo se exige que esta herramienta tenga 4 puertos/slots de tipo 1GE RJ45 o de fibra óptica 1GE SFP, se utilizarán, dos de estos puertos para conectar con los 2 conmutadores en alta disponibilidad. Siendo prioritaria la conexión de fibra óptica, si ambos casos fueran factibles.

4.1) 1ª ópción: conexión a través de fibra óptica 1GE SFP:

- **2** Transceptores SFP Mini-GBIC LC Dúplex Gigabit 1000BASE-SX - Genérico Compatible - DOM - 550m - 850nm.
- Cableado: **2** cables o latiguillos de fibra óptica (multimodo, de banda ancha OM2 o OM3, 1Gigabit-SFP, 850nm), conectores LC Duplex- LC Duplex, de **1** metro.

4.2) 2ª ópción: conexión a través de cable de cobre 1GE RJ45:

- **2** transceptores SFP RJ45 Gigabit 1000Base-T.
- Cableado: **2** cables de Ethernet 1000Base-T de **1** metro.

5) Conexión nuevo core (2 switches) con la herramienta de gestión de logs (en el mismo rack). Dado que como mínimo se exige que esta herramienta tenga 4 puertos/slots de tipo 1GE RJ45 o de tipo 1GE SFP, se utilizarán, dos de estos puertos para conectar con los 2 conmutadores en alta disponibilidad. Siendo prioritaria la conexión de fibra óptica si ambos casos fueran factibles.

5.1) 1ª ópción: conexión a través de fibra óptica 1GE SFP:

- **2** Transceptores SFP Mini-GBIC LC Dúplex Gigabit 1000BASE-SX - Genérico Compatible - DOM - 550m - 850nm.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 22 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- Cableado: **2** cables o latiguillos de fibra óptica (multimodo, de banda ancha OM2 o OM3, 1Gigabit-SFP, 850nm), conectores LC Duplex- LC Duplex, de **1** metro.

5.2) 2ª ópción: conexión a través de cable de cobre 1GE RJ45:

- **2** transceptores SFP RJ45 Gigabit 1000Base-T.
- Cableado: **2** cables de Ethernet 1000Base-T de **1** metro.

Todos los transceptores y el cableado incluidos en este apartado deberán ser compatibles con los dispositivos que conectan. El cableado de fibra óptica deberá contar al menos con una chaqueta de PVC (OFNR riser) resistente a la oxidación y degradación siguiendo el estándar de la industria, y el conector de fibra dúplex cumplirá con TIA/EIA 604-10A para las redes de cableado de alta velocidad.

6. Condiciones de la garantía.

El periodo de garantía mínimo de todo el hardware incluido en la presente contratación será de 2 años (24 meses), a contar desde la firma del acta de recepción de conformidad por parte de CCIU. Obligando dicha garantía a realizar durante este período las sustituciones (totales o parciales) del hardware necesarias para solventar las deficiencias detectadas e imputables a la misma.

Toda actuación de sustitución o reemplazo de algún dispositivo cubierta por la garantía será solicitada por el Responsable del Contrato de CCIU o el responsable técnico en quien delegue a la empresa contratista o al fabricante, que propondrán un plan de actuaciones a aprobar por el primero. En cualquier caso, las actuaciones se llevarán a cabo en los plazos máximos establecidos en el **Cuadro 6**.

CUADRO 6. PLAZOS DE RESOLUCIÓN DE INCIDENCIAS CUBIERTAS POR LA GARANTÍA

Tipo de Dispositivo/Modelo	Plazo (días)
Lote I	
Cortafuegos/Modelo XL	Primer día laborable siguiente
Cortafuegos/Modelo L	Tercer día laborable siguiente
Cortafuegos/Modelo M	Tercer día laborable siguiente
Cortafuegos/Modelo S	Tercer día laborable siguiente
Plataforma de administración centralizada.	Primer día laborable siguiente
Herramienta de gestión de logs	Tercer día laborable siguiente
Firewall a nivel de aplicación (WAF)	Primer día laborable siguiente
Lote II	
Switches o conmutadores de red	Primer día laborable siguiente

Nota: Los plazos se iniciarán desde la comunicación de la incidencia por CCIU a la empresa contratista.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 23 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

En concreto, la garantía del hardware incluirá la subsanación de errores, defectos de fábrica, vulnerabilidades o fallos ocultos del hardware que se pongan de manifiesto en el funcionamiento normal de los dispositivos, o que se descubran mediante pruebas (incluidas pruebas de rendimiento) u otros medios realizados por CCIU.

Asimismo, la garantía del hardware incluirá la subsanación de errores del firmware, del sistema operativo y del software (mantenimiento correctivo) detectados por cualquier medio, relacionados con el funcionamiento básico del dispositivo. Entendiendo por funcionamiento básico aquel que tendría el dispositivo en cuestión sin contratar de forma separada ninguna funcionalidad extra.

Por otra parte, la garantía del hardware incluirá también la subsanación de los errores detectados en la documentación entregada (manuales, guías, etc) en caso de que contenga deficiencias o esté incompleta. En este caso los plazos de resolución de incidencias serán de 5 días laborables.

Por último, la garantía del hardware cubrirá la posibilidad de que los modelos suministrados por la empresa contratista alcancen la fecha final de su vida útil antes de la finalización del periodo de garantía.[16] En ese caso, la empresa contratista estará obligada a reemplazar los dispositivos afectados por otros de un modelo más moderno con las mismas o superiores prestaciones técnicas de la misma marca y fabricante manteniendo las mismas o superiores condiciones de soporte de los modelos reemplazados hasta el final del periodo de garantía.

Los nuevos dispositivos o piezas suministradas para la subsanación de errores o anomalías cubiertas por esta garantía del hardware, deberán entregarse de conformidad con lo exigido en este pliego para con los dispositivos originales.

Las actualizaciones del software facilitadas por el fabricante que estén relacionadas con las funcionalidades adquiridas de forma separada (actualizaciones de los motores antimalware, bases de datos de firmas de virus, etc.) se ajustarán a las condiciones de licencias de uso de cada dispositivo establecidas en este pliego y/o vigentes en cada momento.

Igualmente, el soporte técnico especializado del fabricante se ajustará a las condiciones de vigencia de la licencia de uso del software desplegado en cada dispositivo. Las condiciones mínimas que cubrirá la garantía del software contratado se fijan de la siguiente forma:

- Cortafuegos modelo XL: soporte 24x7x365
- Cortafuegos modelo L: soporte 8x5
- Cortafuegos modelo M: soporte 8x5

16 En este contexto se entenderá por la finalización de la vida útil de un modelo determinado, la fecha oficial en la que el fabricante manifieste que ya no se dará soporte técnico o no facilitarán más actualizaciones periódicas del software, sistema operativo o del firmware de dicho modelo.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 24 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- Cortafuegos modelo S: soporte 8x5
- Herramienta de gestión centralizada: soporte 24x7x365
- Herramienta de análisis de los logs: soporte 24x7x365
- Firewall a nivel de aplicación: soporte 24x7x365

7. Otras especificaciones técnicas de carácter normativo.

7.1. Consideraciones sobre normalización.

Siempre que entre los requisitos mínimos de los dispositivos incluidos en este PPT se exija la conformidad con una norma concreta, el cumplimiento con un estándar o especificación técnica determinada, las empresas licitadoras deberán incluir en la documentación técnica que acompañe a su oferta el certificado de conformidad para el modelo en cuestión emitido por el organismo competente, o en su caso, los resultados de comprobaciones realizadas por laboratorios independientes de reconocido prestigio internacional en materia de ciberseguridad TIC donde se recoja de forma explícita dicha conformidad o cumplimiento.

7.2. Cumplimiento de normas medioambientales, ergonómicas y otras.

Todos los modelos suministrados deberán ser conformes con la normativa vigente de la Unión Europea y española en lo referente a los aspectos ergonómicos, medioambientales, de eficiencia energética, de compatibilidad electromagnética y de reducción de la radiación emitida. En especial, habrá que estar a la regulación siguiente:

- La Directiva 2011/65/UE sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos (RoHS).[17]
- La Directiva 2012/19/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, sobre residuos de aparatos eléctricos y electrónicos. (WEEE)
- El Reglamento nº 1907/2006 del Parlamento Europeo y del Consejo de 18 de diciembre de 2006 sobre el registro, evaluación, autorización y restricciones de las sustancias y preparados químicos (REACH).

17 En su última modificación regulada por la Directiva (UE) 2017/2102 del Parlamento Europeo y del Consejo, de 15 de noviembre de 2017, por la que se modifica la Directiva 2011/65/UE sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 25 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

8. Cumplimiento de la normativa en materia de protección de datos de carácter personal y el ENS.

8.1. Seguridad de los sistemas y cumplimiento del ENS.

En cumplimiento de lo dispuesto en el ENS, las empresas licitadoras incluirán referencia precisa, documentada y acreditativa de que los cortafuegos, la plataforma de administración centralizada, la herramienta de análisis de logs y el WAF incluidos en esta contratación están certificados por el **Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información** con el nivel de "Cualificado".[18]La permanencia en dicho Catálogo deberá mantenerse durante la vigencia de todo el periodo de garantía.

En caso de que alguno de los modelos de los dispositivos citados incluidos en la oferta no estuviesen certificados con el nivel establecido a fecha de fin del plazo de presentación de las ofertas, la empresa contratista dispondrá de un plazo de **6 meses** para obtener dicha certificación. Este plazo se iniciará a la fecha de formalización del contrato y en caso de que al final del periodo estipulado, estos modelos de dispositivos no hubiesen obtenido dicha certificación con el nivel requerido, la empresa contratista deberá sustituirlos, en el plazo improrrogable de 30 días, por otros del mismo fabricante y de igual o superiores prestaciones técnicas que en esa fecha se encuentren efectivamente certificados. La propuesta de sustitución requerirá la aceptación de la misma por el Responsable del Contrato de CCIU.

8.2. Confidencialidad e integridad de la información y protección de datos de carácter personal.

La empresa adjudicataria deberá garantizar la confidencialidad e integridad de los datos de carácter personal manejados, y de la documentación facilitada por CCIU, como consecuencia de la ejecución de los trabajos realizados durante el periodo de garantía. Cuando la información manejada contenga datos de carácter personal, deberá dar cumplimiento a lo establecido en el Reglamento General de Protección de Datos (en adelante RGPD)[19] y a la actual normativa nacional en esta materia en aquellos temas que no contradiga la anterior.[20]

Cualquier duda o cuestión que se plantee en este ámbito, se resolverá siguiendo las instrucciones o directrices de la persona Delegada de Protección de Datos de CCIU.

---

18 El Centro Criptológico Nacional es el Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), según lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

19 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

20 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 26 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

9. Propiedad intelectual.

Toda la documentación técnica generada durante la ejecución de este contrato, incluido el periodo de garantía, será propiedad intelectual exclusiva de CCIU. La empresa contratista no podrá conservarla ni utilizarla o facilitarla a terceros sin la expresa autorización de esta Consejería. Dicha autorización se concederá, en su caso, previa solicitud de la empresa contratista y se circunscribirá exclusivamente a los fines y la duración determinados en la misma.

10. Presupuesto detallado.

El importe de licitación asciende aproximadamente a 180.000 euros (iva incl.). Este importe se ha obtenido analizando los precios actuales del mercado internacional de los principales fabricantes, utilizando el tipo de cambio euro/dólar estadounidense a 2018/09/27 (1 € = 1,1606 $). De este análisis se han extraído los precios aproximados para los distintos dispositivos que se pretenden adquirir junto a las licencias de uso del software más comunes y el soporte técnico especializado del propio fabricante para el periodo de un año. El Presupuesto desglosado por tipo de dispositivo puede consultarse en el **Cuadro 7**:

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 27 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 7. PRESUPUESTO DESGLOSADO.

Dispositivo/Modelo	Precio (€)	Unidades /sede	Sedes	Total Unidades	Total (€)
Cortafuegos/Modelo XL (hardware)	5.700,00	2	1	2	11.400,00
Licencia de uso del software a desplegar en el Modelo XL (1 año)	3.700,00	2	1	2	7.400,00
Cortafuegos/Modelo L (hardware)	1.150,00	2	9	18	20.700,00
Licencia de uso del software a desplegar en el Modelo L (1 año)	750,00	2	9	18	13.500,00
Cortafuegos/Modelo M (hardware)	640,00	2	9	18	11.520,00
Licencia de uso del software a desplegar en el Modelo M (1 año)	360,00	2	9	18	6.480,00
Cortafuegos/Modelo S (hardware)	510,00	1	7	7	3.570,00
Licencia de uso del software a desplegar en el Modelo S (1 año)	240,00	1	7	7	1.680,00
Plataforma de administración centralizada.	24.000,00	1	1	1	24.000,00
Licencia de uso del software a desplegar en la plataforma de administración centralizada (1 año)	4.300,00	1	1	1	4.300,00
Herramienta de gestión de logs	7.400,00	1	1	1	7.400,00
Licencia de uso del software a desplegar en la herramienta de gestión de logs (1 año)	1.300,00	1	1	1	1.300,00
Firewall a nivel de aplicación (WAF)	18.000,00	1	1	1	18.000,00
Licencia de uso del software a desplegar en el WAF (1 año)	8.150,00	1	1	1	8.150,00
Switches o conmutadores de red (incluye cableado de stacking)	4.500,00	2	1	2	9.000,00
Dispositivos de conexión	350,00	1	1	1	350,00
Total (IVA excluido)					148.750,00
IVA (21 %)					31.237,50
Total (IVA incluido)					179.987,50

Anexo I. Modelos descatalogados no susceptibles de ser ofertados.

Fortinet FortiGate (gama baja)	
Fortinet FortiGate-20C Series	Fortinet FortiGate-80C Series
Fortinet FortiGate 20C-ADSL-A	Fortinet FortiGate-80CM Series
Fortinet FortiGate 30B Series	Fortinet FortiGate-80D Series
Fortinet FortiGate-30D Series	Fortinet FortiGate-91E Series
Fortinet FortiGate-30D-POE Series	Fortinet FortiGate-92D Series
Fortinet FortiGate-40C Series	Fortinet FortiGate 110C Series
Fortinet FortiGate-50B Series	Fortinet FortiGate 111C Series
Fortinet FortiGate 51B Series	Fortinet FortiGate 140D Series
Fortinet FortiGate-60C Series	Fortinet FortiGate 140D POE Series
Fortinet FortiGate-60C-POE Series	Fortinet FortiGate 140D POE T1 Series
Fortinet FortiGate-60D-POE Series	Fortinet FortiGate Rugged-100C Series
Fortinet FortiGate-70D Series	Fortinet FortiGateVoice-40D2
	Fortinet FortiGateVoice-70D4 Series
Fortinet FortiGate (gama media)	
Fortinet FortiGate 200B Series	Fortinet FortiGate 400E Series
Fortinet FortiGate 200D Series	Fortinet FortiGate 401E Series
Fortinet FortiGate 200B-POE Series	Fortinet FortiGate 500D Series
Fortinet FortiGate 224B Series	Fortinet FortiGate 620B-DC Series
Fortinet FortiGate 310B-DC Series	Fortinet FortiGate 621B Series
Fortinet FortiGate 311B Series	Fortinet FortiGate 621B-DC Series
Fortinet FortiGate 300C Series	Fortinet FortiGate 800 Series
Fortinet FortiGate 400D Series	Fortinet FortiGate 800F Series
Fortinet FortiGate (gama alta)	
Fortinet FortiGate 1240B-DC Series	Fortinet FortiGate 3600LX4 Series
Fortinet FortiGate 3016B Series	Fortinet FortiGate 3810A Series
Fortinet FortiGate 3240C Series	Fortinet FortiGate 3810A-DC Series
Fortinet FortiGate 3600 Series	Fortinet FortiGate 3950B Series
Fortinet FortiGate 3600A Series	Fortinet FortiGate 5001B Series
Fortinet FortiGate 3600C Series	Fortinet FortiGate 5101C Series

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 29 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Fortinet FortiGate Chassis Platforms:	
FortiGate 5001B	Fortigate-7040E-3
FortiSwitch 5003A	Fortigate-7040E-4
FortiSwitch 5003B	Fortigate-7040E-5
FortiSwitch 5203B	Fortigate-7040E-6
FortiGate 5101C	Fortigate-7040E-DC
Fortigate-7040E-1	Fortigate-7060E-1
Fortigate-7040E-2	Fortigate-7060E-3
FortiManager (herramienta de administración)	
FortiManager 200D	FortiManager 1000C
FortiManager 300D	FortiManager 1000D
FortiManager 400A	FortiManager 3000C
FortiManager 400B	FortiManager 3900E
FortiManager 400C	FortiManager 4000D
	FortiManager 4000E
FortiWeb (WAF)	
FortiWeb 400C	FortiWeb 3000D
FortiWeb 1000C	FortiWeb 3000D-FSX
FortiWeb 3000C	FortiWeb 4000C
FortiWeb 3000C-Fsx	FortiWeb 4000D
FortiAnalyzer (herramienta gestión logs)	
FortiAnalyzer 100B	FortiAnalyzer 3000E
FortiAnalyzer 200D	FortiAnalyzer 3500E
FortiAnalyzer 300D	FortiAnalyzer 4000A
FortiAnalyzer 400C	FortiAnalyzer 3000D
FortiAnalyzer 1000C	FortiAnalyzer 3900E
FortiAnalyzer 1000D	FortiAnalyzer 4000B
FortiAnalyzer 2000B	
Sophos Firewall Manager (herramienta de administración)	
Dispositivo de seguridad FSM 200	Dispositivo de seguridad FSM 400
Dispositivo de seguridad FSM 300	

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 30 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Anexo II. Especificaciones técnicas de los dispositivos.

CUADRO 1. ESPECIFICACIONES TÉCNICAS DE LOS CORTAFUEGOS.

Modelo	XL	L	M	S	Observaciones
Interfaces y módulos (dotación mínima)					
1 GE RJ45 port		2		2	WAN ports
1 GE RJ45 port			1	1	DMZ Ports
1 GE RJ45 port	1/1				MGMT/HA Ports
1 GE RJ45 port		1/1			MGMT/DMZ Ports
1 GE RJ45 port		2	1		HA Ports
1 GE RJ45 port	8	14	12	7	Internal Ports (switch ports)
10 GE SFP+ slot	2				
1 GE SFP slot	8				
1GE RJ45 port/SFP slot		2 pares	2 pares		(Shared Media Pairs)
USB (3.0) ports	2	1	1	1	
Puerto consola	1	1	1	1	
Especificaciones técnicas de rendimiento					
Nivel I estrés:	36/36/22 Gbps	7,4/7,4/4,4 Gbps	4/4/4 Gbps	3/3/3 Gbps	tráfico paquetes UDP (1518/512/64 bytes)
Latencia	2 µs	3 µs	3 µs	3 µs	(1)
Reenvío de paquetes	33 Mpps	6,6 Mpps	6 Mpps	4,5 Mpps	tráfico de paquetes por segundo
Sesiones TCP concurrentes	8 Million	2 Million	1,3 Million	1,3 Million	(2)
Nuevas sesiones TCP/seg.	300.000	30.000	30.000	30.000	(3)
IPsec VPN	20 Gbps	4 Gbps	2,5 Gbps	2 Gbps	(2)
Gateway-to-Gateway IPsec VPN Tunnels	2.000	2.000	200	200	Máximo número de sesiones aconsejable
Client-to-Gateway IPsec VPN Tunnels	50.000	10.000	2.500	500	Máximo número de sesiones aconsejable
SSL-VPN Throughput	5 Gbps	250 Mbps	200 Mbps	150 Mbps	
Concurrent SSL-VPN	500	300	200	100	Máx. sesiones recomendado
Nivel II estrés:	11Gbps/ 5,2Gbps	1,9Gbps/ 500Mbps	1,5Gbps/ 450Mbps	1.400Mbps/ 400Mbps	Rendimiento IPS (HTTP/Enterprise Mix) (3)
SSL Inspection	5,7 Gbps	190 Mbps	180 Mbps	175 Mbps	(4)
Control a nivel de aplicación	14 Gbps	1 Gbps	900 Mbps	650 Mbps	(5)

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 31 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 1. ESPECIFICACIONES TÉCNICAS DE LOS CORTAFUEGOS.

Modelo	XL	L	M	S	Observaciones
Nivel III estrés	5 Gbps	350 Mbps	350 Mbps	250 Mbps	(6)
Nivel IV estrés	4,5 Gbps	250 Mbps	250 Mbps	200 Mbps	(7)
Otras características.					
Políticas permitidas	10.000	10.000	5.000	5.000	Máx núm de políticas permitidas
Dominios Virtuales	10/10	10/10	10/10	10/10	por defecto/máximo
Máximo núm. de puntos de acceso inalámbrico	512/256	64/32	32/16	30/10	(total/modo túnel)
Configuración en alta disponibilidad.	Activo / Activo Activo / Pasivo				
Switches soportados	48	24	8	8	Núm. máximo
Dimensiones					
Formato compacto	(altura) 1U				Montable en rack de 19" (con o sin accesorios)
Accesorios a incluir obligatoriamente en la oferta					
Dispositivo de suministro redundante de energía eléctrica externo,	SI	SI	NO	NO	intercambiable en caliente
Transceptores fibra óptica compatibles 10GE SFP+	4				(2 por dispositivo) del tipo: 10 GE SFP + (10GBase-SR) Conector LC-Duplex
Cable conexión puerto consola	1	1	1	1	

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 32 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

NOTAS RELATIVAS A LAS ESPECIFICACIONES TÉCNICAS DE RENDIMIENTO DEL CUADRO 1.

1. Prueba realizada con paquetes UDP de 64 bytes. Con un máximo de 1.488.000 tramas por segundo por 1 Gigabit de tráfico.
2. Esta prueba determina las conexiones TCP simultáneas máximas del cortafuegos sin que los datos pasen a través de las conexiones.
3. Para realizar esta prueba se establece un número cada vez mayor de sesiones nuevas a través del cortafuegos para determinar el punto exacto de fallo. Cada sesión se abre normalmente, un byte de datos se pasa al dispositivo y luego la sesión se cierra inmediatamente. La carga aumenta hasta que se alcanza uno o más de los puntos de ruptura definidos anteriormente.
4. El rendimiento **IPsec VPN** se ha establecido para un tráfico encriptado con AES256+SHA256 utilizando paquetes UDP de 512 bytes.
5. Las cifras relativas al rendimiento establecido para la funcionalidad **IPS**, se refieren a dos contextos distintos: el primero (óptimo) utilizando exclusivamente tráfico HTTP de 1 Mbyte y el segundo con un tráfico acorde al estándar *Enterprise Traffic Mix* con el sistema de logs activado.
6. Para el modelo XL: el rendimiento en la inspección del tráfico SSL (**SSL Inspection Throughput**) se ha establecido con la funcionalidad IPS activada y con un tráfico HTTPS procedente de diversas fuentes.
Para los modelos L, M: el rendimiento en la inspección del tráfico SSL se ha establecido con la funcionalidad IPS activada y con un tráfico HTTPS utilizando TLS v1.2 con AES128-SHA256.
7. El rendimiento de la funcionalidad **Application Control** se ha establecido con un tráfico HTTP de 64 Kbytes y con el sistema de logs activado.
8. El rendimiento del **Nivel III** de estrés se ha establecido con la funcionalidades Firewall "tradicional", IPS y Application Control activadas, con el sistema de logs activado y con un tráfico basado en el estándar *Enterprise Traffic Mix*.
9. El rendimiento del **Nivel IV** de estrés se ha establecido con las funcionalidades Firewall "tradicional", IPS, Application Control y Malware protection activadas, con el sistema de logs activado y con un tráfico basado en el estándar *Enterprise Traffic Mix*.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 33 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 2. RESUMEN DE LAS ESPECIFICACIONES TÉCNICAS DE LA PLATAFORMA DE GESTIÓN CENTRALIZADA.

Concepto	Valor	Observaciones
Especificaciones del hardware		
1GE RJ45 Ports/SFP 1GE slots	4/0	Mínimo 4 puertos de 1GE en cualquier combinación de puertos RJ45 y/o slots de fibra óptica siempre que dos puertos al menos sean iguales
	2/2	
	0/4	
Capacidad de almacenamiento	12 TB	(4 discos x 3 TB)
Niveles RAID soportados	RAID 0/1/5/10	
USB (3.0) ports	2	
Puerto consola	1	
Otras Especificaciones		
Dispositivos	100	mínimo a administrar
Formato compacto	Altura 1U	Montable en rack de 19”
Accesorios a incluir obligatoriamente en la oferta		
El cable de conexión al puerto consola.	1	
Transceptores compatibles SFP 1GE conector LC Duplex	2	En las combinaciones siguientes: 2/2 o 0/4

Nota: 2 de los 4 puertos 1GE conectarán con el nuevo core de conmutadores en HA. Prioritariamente a través de fibra óptica con los transceptores SFP 1GE en caso de que el dispositivo cuente con ellos.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 34 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 3. RESUMEN DE LAS ESPECIFICACIONES TÉCNICAS DE LA HERRAMIENTA DE GESTIÓN CENTRALIZADA DE LOGS.

Concepto	Valor	Observaciones
Especificaciones relativas al rendimiento		
Capacidad de procesamiento diario de logs (GB/día)	150	
Núm. análisis diarios almacenados en el sistema.	25	dividir la capacidad de almacenamiento real entre el máximo de GB procesados al día (4000/15 = 26,7 días)
Capacidad de almacenamiento	8 TB	(2 discos x 4 TB)
Capacidad de almacenamiento útil	4 TB	(después del RAID 1)
Niveles RAID soportados	RAID 0/1	
Especificaciones del hardware		
1GE RJ45 Ports/SFP 1 GE slots	4/0	Mínimo 4 puertos de 1GE en cualquier combinación de puertos RJ45 y/o slots de fibra óptica siempre que dos puertos al menos sean iguales
	2/2	
	0/4	
USB (3.0) ports	2	
Puerto consola	1	
Otras Especificaciones		
Formato compacto	altura 1U	Montable en rack de 19”
Dispositivos analizados (núm. mínimo)	180	
Accesorios a incluir obligatoriamente en la oferta		
El cable de conexión al puerto consola.	1	
Transceptores compatibles SFP 1GE conector LC Duplex	2	En las combinaciones de puertos siguientes: 2/2 o 0/4

Nota: 2 de los 4 puertos 1GE conectarán con el nuevo core de conmutadores en HA. Prioritariamente a través de fibra óptica con los transceptores SFP 1GE en caso de que el dispositivo cuente con ellos.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 35 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 4. RESUMEN DE LAS ESPECIFICACIONES TÉCNICAS DEL FIREWALL A NIVEL DE APLICACIÓN (WAF).

Concepto	Valor	Observaciones
Especificaciones relativas al rendimiento		
Rendimiento	1,3 Gbps	Nivel mínimo del rdto máximo en condiciones òptimas
Latencia	Sub-ms	
Especificaciones del hardware		
1GE RJ45 Ports	6	(4 bypass)
SFP 1GE slots	4	(non bypass)
10G BASE-SR SFP+ slots	2	
Capacidad de almacenamiento	4 TB	(2 discos x 2 TB)
USB (3.0) ports	2	
Puerto Consola	1	
Otras Especificaciones		
Formato compacto	altura máxima 2U	
Suministro energía	Doble intercambiable en caliente	
Alta disponibilidad	Activo/Activo Activo/Pasivo	
Dominios Administrativos	64	
Accesorios a incluir obligatoriamente en la oferta		
El cable de conexión al puerto consola.	1	
Transceptores compatibles 10G SFP+ (10GBase-SR) conector LC-Duplex	2	

Nota: Los 2 puertos de alta velocidad 10G SFP+ conectarán con el nuevo core de conmutadores en HA

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 36 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

CUADRO 5. RESUMEN DE LAS ESPECIFICACIONES TÉCNICAS DE LOS SWITCHES O CONMUTADORES DE RED.

Concepto	Valor	Observaciones
Especificaciones relativas al rendimiento		
Capacidad de transmisión.	2,56 Tbps	
Rendimiento de reenvío de paquetes.	720 Mpps	
Latencia	< 1µs	Latencia promedio máxima
Tabla de direcciones MAC (entradas de direcciones MAC)	288.000	Aprendizaje y vencimiento de direcciones MAC Entradas de direcciones MAC estáticas, dinámicas y blackhole Filtrado de paquetes en función de las direcciones MAC de origen
Especificaciones del hardware		
10 GE SFP+ slots	24	Los slots 10 GE SFP+ deben ser compatibles con 1GB SFP
40 GE QSFP+	2	Posibilidad de apilamiento mediante puertos de servicio de 40G (2 puertos 40G QSFP+), con configuración unificada.
Puerto Consola	1	
Ranuras extendidas	1	Una ranura extendida para 4 tarjetas de interfaces 40 GE QSFP+
Puerto USB (3.0)	1	
Otras Especificaciones		
Formato compacto	1U Montable en rack de 19"	
Suministro energía	Doble fuente de alimentación intercambiable en caliente.	
Tipo de administración	Posibilidad de configuración mediante línea de comandos (SSH) y mediante interfaz web (HTTPS).	
Accesorios a incluir obligatoriamente en la oferta		
El cable de conexión al puerto consola.	2	
Cableado de stacking 2 puertos 40G QSFP+	2	
Transceptores compatibles 10G SFP+ (10GBase-SR) Conector LC-Duplex	10	Conexión mediante fibra óptica de alta velocidad 10G SFP+ con los dos cortafuegos XL (4 transceptores), con el WAF (2 transceptores) y con el core de conmutadores actual (4 transceptores).
Transceptores compatibles 1GE SFP Conector LC-Duplex	4	Conexión prioritaria con la herramienta de administración centralizada y con la herramienta de gestión de logs mediante fibra óptica 1GE SFP en HA.
Transceptores compatibles 1GE RJ45	4	Conexión alternativa con la herramienta de administración centralizada y con la herramienta de gestión de logs mediante cableado de cobre 1GE RJ45 en HA

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 37 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Anexo III: Glosario de términos, acrónimos y abreviaturas.

- ADOM Dominio de Administración. En este contexto se trata de conjuntos de dispositivos agrupados o clasificados por uno o varios criterios. Los administradores de red pueden controlar mejor sus redes agrupando sus dispositivos en dominios de administración, aplicando políticas de forma más eficiente y distribuyendo actualizaciones de firmware y contenidos de seguridad.
- AES siglas en inglés de *Advanced Encryption Standard* es un estándar de cifrado por bloques usado en criptografía simétrica..
- APP Arquitectura de protección perimetral.
- CBHL Catálogo de Bienes Homologados de la Junta de Andalucía.
- CCIU: Consejería de Conocimiento, Investigación y Universidad.
- CEC: Consejería de Economía y Conocimiento (extinta).
- CEEC: Consejería de Empleo, Empresa y Comercio.
- CEHAP: Consejería de Economía, Hacienda y Administración Pública de la Junta de Andalucía.
- CPD: Centro de Proceso de Datos.
- CRIJA Censo de Recursos Informáticos de la Junta de Andalucía.
- DDOS: siglas en inglés de *Distributed Denial of Service, l*a traducción es "ataque distribuido denegación de servicio", ataque a un servidor desde muchos ordenadores para que deje de funcionar.
- DDTT: Delegaciones Territoriales de Conocimiento y Empleo dependientes orgánicamente de CCIU.
- Enterprise Traffic Mix: Según la IETF se trata de un estándar que simula un tráfico compuesto de un 30% de tráfico HTTP y un 70% de tráfico HTTPS de una combinación de aplicaciones y sitios web como Facebook, WhatsApp, Dropbox, Office 365, etc.
- ENS: Esquema Nacional de Seguridad.
- Fecha de descatalogación: fecha de compra final.
- Fecha de última renovación: última oportunidad para ampliar servicios de suscripción, garantía y soporte técnico. Las ampliaciones de soporte ya no serán posibles tras la fecha de fin de vida útil del producto.
- Fin de vida útil: fecha en la que finaliza el soporte para el producto.
- GE: Gigabit Ethernet es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 38 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- IETF: siglas en inglés de la *Internet Engineering Task Force*, una amplia comunidad internacional abierta formada por investigadores, proveedores, operadores y diseñadores de redes interesados en la evolución de la arquitectura de Internet y su funcionamiento libre de complicaciones.
- IPS: siglas en inglés de *Intrusion Prevention System*. Un sistema de prevención de intrusos es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.
- Júpiter: Sistema Integrado de Gestión Presupuestaria, Contable y de Tesorería de la Junta de Andalucía.
- LAN: red de área local.
- Listado de Productos Aprobados: son productos cuyo uso está aprobado en sistemas que manejen información clasificada.
- Listado de Productos Cualificados: son productos que tienen certificadas sus funcionalidades de seguridad y, por lo tanto, son aptos para ser utilizados en sistemas afectados por el ENS que hayan sido etiquetados como Categoría ALTA por requerir un nivel alto de seguridad en cualquiera de sus dimensiones (Confidencialidad, Disponibilidad, Integridad, Trazabilidad y Autenticidad).
- MB: megabyte.
- NAT: del inglés *Network Address Translation* o traducción de direcciones de red, también llamado enmascaramiento de IP, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.
- NGFW: siglas en inglés de New Generation Firewalls, firewalls de nueva generación que son capaces de detener los ataques externos mediante la inspección de tráfico avanzada y la detección y control de aplicaciones y usuario (independientemente de los protocolos/puertos usados).
- OWASP: en inglés *Open Web Application Security Project*, en español Proyecto Abierto de Seguridad de Aplicaciones Web.
- OWASP top 10: es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP. Esta lista se publica y actualiza cada tres años por dicha organización.
- PCAP: Pliego de Cláusulas Administrativas Particulares.
- PPT: Pliego de Prescripciones Técnicas.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 39 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- RCJA: Red Corporativa de Telecomunicaciones de la Junta de Andalucía.
- RFID: Siglas en inglés de "*Radio Frequency IDentification*", es decir, Identificación por Radiofrecuencia.
- RoHS: (de las siglas en inglés *Restriction of Hazardous Substances*) se refiere a la directiva 2002/95/CE de Restricción de ciertas Sustancias Peligrosas en aparatos eléctricos y electrónicos, adoptada en febrero de 2003 por la Unión Europea.
- SANDETEL: Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, S.A.
- SFP: del inglés *small form-factor pluggable*, se usa para definir un transceptor compacto y conectable en caliente utilizado para las aplicaciones de comunicaciones de datos y telecomunicaciones
- SO: Sistema Operativo.
- SSCC: Servicios Centrales de la Consejería de CCIU.
- TB: Terabyte. Equivalente a 10^{12} bytes
- UTM: siglas en inglés de *Unified Threat Management* o Gestión Unificada de Amenazas, es un término que se refiere a un dispositivo de red único con múltiples funciones, las funcionalidades básicas que suelen tener son: antivirus, firewall (cortafuegos) y un sistema de detección/prevención de intrusos. En el argot de la ciberseguridad a veces se utiliza para hacer referencia a los cortafuegos de nueva generación de gama baja-media.
- WAF: las siglas en inglés de *Web Application Firewall*. Es un dispositivo que filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Puede filtrar el contenido de aplicaciones web. Mientras un firewall tradicional de red protege tráfico entre los servidores, un WAF protege páginas de una aplicación web contra ataques como inyección SQL, XSS y falsificación de petición de sitios cruzados (CSRF) por el inspector del protocolo HTTP.
- WAN: red de área amplia.
- WEEE: (Del inglés *Waste Electrical and Electronic Equipment*). La Directiva de Residuos de Aparatos Eléctricos y Electrónicos, 2002/96/CE, entró en vigor el 13 de agosto del 2005 en todo el ámbito de la Unión Europea. Pretende promover el reciclaje, la reutilización y la recuperación de los residuos de estos equipos para reducir su contaminación. En 2012 fue sustituida por la Directiva 2012/19/UE del Parlamento Europeo y del Consejo.

Fuente:

https://es.wikipedia.org

https://datatracker.ietf.org/meeting/101/materials/slides-101-bmwg-firewall-benchmarking-for-modern-firewalls-00

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 40 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Anexo IV. Procedimiento de inventariado de bienes no homologados.

1. Objeto.

El presente documento define de forma procedimental las acciones que deberán llevar a cabo todos los proveedores que suministren equipos informáticos a las Consejerías u Organismos de la Junta de Andalucía para el etiquetado e inventariado de estos bienes. Estos equipos informáticos formarán parte del Censo de Recursos Informáticos de la Junta de Andalucía (en adelante CRIJA) y como tal, estarán identificados con una etiqueta RFID con un código que estará recogido en la base de datos de del citado sistema de información.

2. Alcance.

El alcance de este procedimiento es de aplicación para el inventario de bienes informáticos de la Junta de Andalucía. Este documento será aplicable a todos los proveedores que suministren bienes informáticos a la Junta de Andalucía no incluidos en el CBH.

3. Requisitos mínimos que debe cumplir el proveedor.

Para realizar el etiquetado, el proveedor deberá disponer al menos de:

Un terminal de lectura de etiquetas RFID compatible con la normativa ETSI EN 300 220 (868 MHz, 500 mW de potencia de salida).

Disponer de acceso con un perfil adecuado a la aplicación de CRIJA publicada en el URL:

http://crijaglpi.i-administracion.junta-andalucia.es/proveedores/

4. Secuencia de actividades para el inventariado de bienes informáticos.

- **Paso 1** (Notificación de compra).

La Consejería u Organismo expresa su necesidad de adquirir equipos informáticos que no están en el CBH de la Junta de Andalucía, por lo que genera un expediente de compra de equipos.

- **Paso 2** (Inserción de datos en CRIJA).

El proveedor asociado al expediente deberá acceder al módulo correspondiente de la aplicación CRIJA e incorporar la siguiente información relacionada con los bienes a servir:

  - Marcas y modelos.
  - Número de serie de los equipos.
  - Características técnicas asociadas a los equipos.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 41 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

- Relación de sedes en donde se entregarán los equipos.
- Fecha de suministro prevista.
- Fecha de garantía de los equipos.

Más adelante se describe el procedimiento de inserción de datos en CRIJA.

- **Paso 3** (Generación etiquetas RFID).

CEHAP generará provisionalmente los números de inventario de patrimonio. A continuación, SANDETEL generará las etiquetas RFID que incluirá el número de inventario de patrimonio de cada equipo e informará al proveedor cuando puede recogerlas. Junto con las etiquetas, SANDETEL entregará un listado en formato electrónico donde se asociará cada número de inventario de patrimonio (codificado en la etiqueta RFID) con el número de serie del equipo, de tal forma que el proveedor pueda etiquetar fácilmente todos los equipos.

- **Paso 4** (Etiquetado de equipos).

El proveedor etiquetará los equipos con las etiquetas proporcionadas por SANDETEL de acuerdo al procedimiento de etiquetado descrito en este Anexo.

- **Paso 5** (Verificación del etiquetado).

El proveedor deberá verificar el correcto etiquetado de los equipos con un Terminal de Mano RFID. SANDETEL, se reserva el derecho de realizar una verificación posterior en las instalaciones del proveedor tal y como se describe en este Anexo.

- **Paso 6** (Entrega de los equipos)

El proveedor entregará los equipos correctamente etiquetados en las instalaciones de la Consejería u Organismo que se indicaron en el paso 2.

5. Procedimiento de etiquetado de los equipos por parte del proveedor.

SANDETEL proporcionará al proveedor las etiquetas RFID necesarias para su colocación en todos los equipos inventariables que va a suministrar. Para ello, SANDETEL contactará con el proveedor por correo electrónico y/o teléfono a través de los datos de contacto registrados en CRIJA, informándole de la fecha a partir de la cuál el proveedor podrá recoger las etiquetas. El lugar de recogida será: SANDETEL. Avda. Camino de los Descubrimientos, n.º 17 Planta -1 (Sótano). Pabellón de Francia – Isla de la Cartuja. 41092 Sevilla.

Para la recogida de las etiquetas, el proveedor deberá presentar el código del expediente del suministro.

Para el proceso de etiquetado por parte del proveedor, se deberá seguir el siguiente procedimiento:

- Leer la etiqueta antes de su colocación en el equipo con el Terminal de Lectura RFID. Para ello,

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 42 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

deberá aislar la etiqueta de otras etiquetas RFID para evitar múltiples lecturas. Si su lectura es satisfactoria, se procederá al pegado de la etiqueta en el equipo. En el caso de que la lectura fallara, se deberá marcar como defectuosa, registrándose esta incidencia en un listado de etiquetas defectuosas. Posteriormente, el proveedor enviará a SANDETEL las etiquetas defectuosas conjuntamente con el listado de etiquetas defectuosas para que se proceda a la creación de unas nuevas etiquetas.

- Limpiar cuidadosamente la zona sobre la que se realizará la colocación de la etiqueta. Si se realiza la colocación de una etiqueta RFID sobre un equipo en una zona cubierta por una capa de polvo, la adherencia del pegamento de la etiqueta será menor, pudiendo ésta llegar a despegarse.
- Secar adecuadamente la zona sobre la que se realizará la colocación de etiquetas en los casos en los que se utilicen productos líquidos para la limpieza. Del mismo modo que el polvo puede influir sobre la adherencia de una etiqueta, colocar la etiqueta sobre una zona húmeda puede provocar que ésta llegue a despegarse.
- Evitar colocar la etiqueta en una parte metálica del equipo, ya que impide la posterior lectura RFID de la etiqueta.
- Colocar la etiqueta en una parte del equipo que sea visible a simple vista, como en el frontal de un monitor, parte visible de un PC de sobremesa, etc.
- No colocar la etiqueta en partes del equipo que sean sustituibles o no sean fijas (bahías de un ordenador de sobremesa, base de un monitor TFT, batería de un ordenador portátil, bandejas de impresoras, etc), evitando la pérdida posterior de la etiqueta por reparación o sustitución de un módulo en el equipo.
- Colocar la etiqueta siempre alejada de fuentes de calor.
- Evitar su colocación cerca de circuitos electrónicos con alta concentración de metal.
- Anotar los datos del equipo etiquetado (número de serie y sede de destino) para posteriormente realizar el emparejamiento en CRIJA con el número de inventario codificado en la etiqueta.
- Para el etiquetado de un equipo nuevo o similar a otro que ya ha sido etiquetado correctamente pero de diferente marca y/o modelo, comprobar, previo al etiquetado, la lectura correcta de la etiqueta en el lugar deseado para la colocación de la misma. Para ello, se podrá solicitar a SANDETEL etiquetas de pruebas que deberán adherirse al lugar deseado del dispositivo usando otro medio distinto al adhesivo de la propia etiqueta (cinta adhesiva, por ejemplo), evitando de esta forma cualquier daño en el equipo por la retirada posterior de la etiqueta de prueba.
- En el caso que surja alguna duda durante el proceso de etiquetado, consultar al personal de SANDETEL enviando un correo electrónico a cau.mantenimiento@juntadeandalucia.es describiendo la

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 43 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

consulta e indicando en el asunto "Incidencia etiquetado expediente 'CODIGO EXPEDIENTE DEL SUMINISTRO' " y/o llamando al teléfono: 954544431

6. Procedimiento de inserción de datos en CRIJA por parte del proveedor.[21]

Previo a la inserción de datos en CRIJA, el proveedor deberá recoger las etiquetas RFID generadas por SANDETEL y adherirlas a los equipos inventariables objeto del suministro, anotando el número de serie y sede de destino del equipo etiquetado con el objeto de facilitar el emparejamiento posterior de esta información en CRIJA.

La información que el proveedor deberá insertar en CRIJA es la siguiente:

- Número de serie de los equipos.
- Características técnicas asociadas a los equipos. En el caso de suministro de CPU, deberá insertarse el tipo de procesador, de acuerdo al listado existente en CRIJA.
- Marca y modelo de los bienes. Para ello, deberá seleccionar las marcas y modelos del listado existente en CRIJA.
- Fecha de suministro prevista.
- Fecha de garantía de los equipos.

Para la inserción de esta información, el proveedor dispondrá de dos opciones:

- Opción 1: Conectar a CRIJA con sus códigos de identificación (certificado digital expedido por la FNMT) y registrar "online" toda la información requerida.
- Opción 2: Conectar a CRIJA y aportar toda la información mediante el uso de un fichero csv normalizado.

Una vez introducidos correctamente todos los datos de los equipos, el proveedor deberá confirmar toda la información en el sistema CRIJA, comenzando a partir de ese momento el proceso de generación de etiquetas RFID para este expediente por parte de SANDETEL. Una vez confirmados los datos, el expediente quedará bloqueado y el proveedor no podrá modificar los registros (únicamente podrá consultar la información en el sistema).

7. Verificación del etiquetado.

El proveedor deberá verificar por sus propios medios la correcta lectura y colocación de las etiquetas en todos los equipos que va a suministrar. SANDETEL se reserva el derecho de realizar inspecciones en las instalaciones del proveedor o en el destino final del equipo para verificar la correcta lectura y colocación del

21 Para la inserción de datos en CRIJA, consultar el "Manual de Usuario de CRIJA para Proveedores".

etiquetado. Cualquier equipo mal etiquetado será rechazado, por lo que el proveedor deberá proceder nuevamente al etiquetado del mismo asumiendo todos los costes generados en el nuevo proceso de etiquetado desde la retirada del equipo hasta la nueva entrega en las sedes de las Consejerías u Organismos.

8. Entrega y validación del etiquetado.

Después del proceso de verificado del etiquetado, el proveedor deberá entregar los equipos en las direcciones de las sedes indicadas en el expediente de suministro. Una vez entregados los equipos, se procederá a la validación del suministro por parte de la Consejería u Organismo correspondiente.

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 45 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	

Anexo V. Sedes incluidas en la Primera Fase del Programa de Securización Perimetral de CCIU.

TIPO	CÓDIGO	NOMBRE SEDE	VÍA	DIRECCIÓN	Nº	CP	MUNICIPIO
L	CEC-ALM-001	DELEGACIÓN TERRITORIAL DE CE EN ALMERÍA	C/	HERMANOS MACHADO	4	04004	ALMERÍA
M	CEC-ALM-003	SERVICIO DE COMERCIO	C/	GERONA	18	04071	ALMERÍA
L	CEC-CAD-001	DELEGACIÓN TERRITORIAL DE CE EN CÁDIZ	Plaza	BLAS INFANTE (EDIFICIO ASDRÚBAL)	S/N	11008	CÁDIZ
M	CEC-CAD-004	SERVICIO DE FORMACION PARA EL EMPLEO		EDIFICIO GLORIETA, ZONA FRANCA		11011	CÁDIZ
M	CEC-COR-001	DELEGACIÓN TERRITORIAL DE CE EN CORDOBA	C/	MANRIQUES	2	14003	CÓRDOBA
L	CEC-COR-002	DELEGACIÓN TERRITORIAL DE CE EN CORDOBA	C/	SANTO TOMÁS DE AQUINO	S/N	14004	CÓRDOBA
S	CEC-COR-003	ARCHIVO DELEGACIÓN TERRITORIAL DE CE EN CÓRDOBA	C/	MARÍA CASTIELLA (ANTIGUA CALLE PROFESOR ARNOLD J. TOYNBEE - P.I. CHINALES)	S/N	14007	CÓRDOBA
S	CEC-COR-006	SALA DE ARCHIVOS	C/	IMPRENTA DE LA ALBORADA (PARC. 110)	3	14014	CÓRDOBA
M	CEC-COR-007	SERVICIO DE FORMACION PARA EL EMPLEO	C/	DOLORES IBARRURI (LOCAL. ENTRADA POR CALLE MARÍA MALIBRÁN)	1	14011	CÓRDOBA
M	CEC-COR-009	S.G.EMPLEO, SERVICIO DE ADMON LABORAL, CMAC, COMERCIO	Avda.	GRAN CAPITÁN	12	14008	CÓRDOBA
L	CEC-GRA-001	DELEGACIÓN TERRITORIAL DE CE EN GRANADA	C/	JOAQUINA EGUARAS (EDIFICIO ALMANJAYAR)	2	18013	GRANADA
S	CEC-GRA-004	SERVICIO DE COMERCIO	Avda.	DE MADRID	7	18012	GRANADA
M	CEC-GRA-006	SERVICIO DE FORMACION PARA EL EMPLEO	Avda.	JOAQUINA EGUARAS (EDIFICIO VICTORIA), LOCALES: 5-12		18013	GRANADA
L	CEC-HUE-001	DELEGACIÓN TERRITORIAL DE CE HUELVA Y CENTRO FIJO DE FORMACION	Camino	SALADILLO	S/N	21007	HUELVA
S	CEC-HUE-003	SERVICIO DE COMERCIO	Avda.	MARTÍN ALONSO PINZÓN	7	21003	HUELVA
L	CEC-JAE-001	DELEGACIÓN TERRITORIAL DE CE EN JAEN	Paseo	DE LA ESTACIÓN (SAC)	19	23007	JAÉN
S	CEC-JAE-003	SERVICIO DE ADMINISTRACIÓN LABORAL	Paseo	DE LA ESTACIÓN	30	23008	JAÉN
S	CEC-JAE-007	SERVICIO DE FORMACION PARA EL EMPLEO	Paseo	DE LA ESTACIÓN	42	23008	JAÉN
L	CEC-MAL-001	DELEGACIÓN TERRITORIAL DE CE EN MALAGA	Avda.	JUAN XXIII	82	29006	MÁLAGA
M	CEC-MAL-002	SERVICIO DE FORMACION PARA EL EMPLEO	C/	MAURICIO MORO	4	29006	MÁLAGA
M	CEC-MAL-003	SERVICIO DE COMERCIO	Avda.	DE LA AURORA	47	29002	MÁLAGA
L	CEC-SEV-001	SERVICIOS CENTRALES CCIU (EDIFICIO KEPLER)	C/	JOHANNES KEPLER (PARCELA TA-7.1 DEL PARQUE TECNOLÓGICO - ISLA DE LA CARTUJA)	S/N	41092	SEVILLA
L	CEC-SEV-004	DELEGACIÓN TERRITORIAL DE CE EN SEVILLA	Avda.	DE GRECIA (EDIFICIO ADMINISTRATIVO BERMEJALES)	S/N	41012	SEVILLA
S	CEC-SEV-005	SALA DEL CONSEJO DE CCIU EN EL PARLAMENTO	C/	PARLAMENTO DE ANDALUCÍA	S/N	41009	SEVILLA
XL	CEC-SEV-010	NUEVO CPD DE CCIU	Avda.	DE LA ARBOLEDA	S/N	41940	TOMARES

ROSA MARIA GOMEZ TORRALBO		06/11/2018	PÁGINA 46 / 46
VERIFICACIÓN	NJyGw6K0O04q6ryZbLohEWj8h3j14X	https://ws050.juntadeandalucia.es/verificarFirma	