Andalucía se mueve con Europa

Pliego de Prescripciones Técnicas

SISTEMA DE CORTAFUEGOS PARA DISTINTAS SEDES DE LA CONSEJERÍA DE SALUD y FAMILIAS

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

JUNTA DE ANDALUCIA

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 1 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 2 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

Índice de contenido

1 INTRODUCCIÓN....5
2 OBJETO DE LA CONTRATACIÓN....6
3 REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ENS....7
3.1 Nuevo Reglamento Europeo de Protección de Datos (Reglamento (UE) 2016/679)....7
3.2 R.D 3/2010 Esquema Nacional de Seguridad (ENS)....7
4 DESCRIPCIÓN DEL ENTORNO TECNOLÓGICO ACTUAL....8
5 DESCRIPCIÓN DEL SUMINISTRO Y LOS SERVICIOS SOLICITADOS....8
5.1 CARACTERÍSTICAS GENERALES....8
5.1.1 IDENTIFICACIÓN Y TRAZABILIDAD DE APLICACIONES....8
5.1.2 IDENTIFICACIÓN DE USUARIOS....9
5.1.3 GESTIÓN Y ADMINISTRACIÓN....9
5.1.4 SEGURIDAD....9
5.1.5 SERVICIOS DE RED....10
5.1.6 OBTENCIÓN Y GESTIÓN DE INFORMES Y LOGS....11
5.2 CLUSTER DE CORTAFUEGOS DE SSCC....11
5.2.1 CAPACIDAD Y RENDIMIENTO DE CADA NODO....12
5.2.2 OTRAS CARACTERÍSTICAS FÍSICAS....12
5.3 CORTAFUEGOS PARA EL SISTEMA DE ALMACENAMIENTO SERVICIO DE HOSTING....13
5.4 INFRAESTRUCTURA DE RED....13
5.5 SISTEMAS DE CORTAFUEGOS Y HERRAMIENTAS DE SEGURIDAD PARA LAS DD.TT....13
5.6 INTEROPERABILIDAD TECNOLÓGICA....14
5.6.1 ADAPTACIÓN AL ESQUEMA NACIONAL DE INTEROPERABILIDAD....14
5.7 PLAN DE DESPLIEGUE....14
5.8 INSTALACIÓN Y CONFIGURACIÓN....15
5.8.1 LA INGENIERÍA DE PUESTA EN FUNCIONAMIENTO Y ARRANQUE....16
5.8.2 LA INSTALACIÓN DEL HARDWARE Y SOFTWARE OFERTADO....16
5.8.3 MIGRACIÓN DE LA POLÍTICA ACTUAL....17
5.8.4 MONITORIZACION DE LA INFRAESTRUCTURA....17
5.8.5 TRANSFERENCIA DEL CONOCIMIENTO....17
5.9 SERVICIO DE ADMINISTRACIÓN DE LA PLATAFORMA....18
5.9.1 CONDICIONES DE PRESTACION DEL SERVICIO....18
5.9.2 COMPOSICION DEL EQUIPO....19
5.9.3 TASACION DEL SERVICIO....19
6 CONDICIONES GENERALES DE EJECUCIÓN Y SUMINISTRO....20
6.1 LUGAR DE EJECUCIÓN DE LOS TRABAJOS....20
6.2 PROCEDIMIENTOS DE TRABAJO....20
6.3 MEDIOS MATERIALES Y HUMANOS....20
6.4 INSTALACIÓN Y PUESTA EN MARCHA....20
6.5 PLANES DE CONTINGENCIA Y GARANTÍA DE CONTINUIDAD DEL SERVICIO....21
6.6 PROCEDIMIENTO DE ETIQUETADO E INVENTARIADO DE BIENES....21
6.7 MEDIDAS DE INFORMACIÓN Y PUBLICIDAD (fondos FEDER)....21
6.8 CONFIDENCIALIDAD DE LA INFORMACIÓN....21
6.9 PROPIEDAD INTELECTUAL DE LOS TRABAJOS....22
7 PLAZOS, TASACION Y FACTURACION DEL PROYECTO....22
7.1 PLAZOS DE SUMINISTRO Y PUESTA EN FUNCIONAMIENTO....22
7.2 TASACION Y FACTURACION DEL PROYECTO....23
8 LICENCIAMIENTO Y GARANTÍA....24

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 3 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

8.1 CARACTERISTICAS GENERALES....24
8.2 ATENCION REMOTA DE CUESTIONES, DUDAS Y CASOS DE SOPORTE....25
8.3 BOLSA HORARIA....25
8.4 CASO ESPECIAL DE FIRMWARE Y ACTUALIZACIONES....25
8.5 RENOVACIONES DE LICENCIAS Y GARANTÍA....25
9 ACUERDO DE NIVELES DE SERVICIO....26
9.1 INSTALACIÓN Y CONFIGURACIÓN....26
9.2 ADMINISTRACION DE LA PLATAFORMA....26
9.3 GARANTÍA....27
10 MEJORAS....28
10.1 CARACTERÍSTICAS DE SANDBOX....28
ANEXO 1. SISTEMA DE CORTAFUEGOS EN SSCC....30
ANEXO 2. SISTEMA DE CORTAFUEGOS EN HOSTING....31
ANEXO 3. SISTEMA DE CORTAFUEGOS EN DD.TT....32
ANEXO 4. PLAN DE PRUEBAS....34
ANEXO 5. SEDES Y LUGARES DE REALIZACIÓN DEL TRABAJO....35
ANEXO 7. PLAN DE CONTINGENCIA....37

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 4 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

1 INTRODUCCIÓN

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público obligan a un cambio de orientación significativo en la prestación de los servicios que las Administraciones ofrecen a los ciudadanos.

La Junta de Andalucía se halla en un proceso que conduce a la adaptación de todas las actuaciones administrativas a lo dispuesto en las leyes 39/2015 y 40/2015, que exigen la existencia de tramitación telemática para los procedimientos ofertados por la Consejería de Salud.

La Consejería de Salud y Familias (CSAFA) se encuentra desarrollando su plan de telematización que constituye el marco de referencia en el que se defina los proyectos que sean necesarios para crear nuevos sistemas de información y realizar los cambios necesarios en los sistemas de información existentes, con objeto de cumplir lo dispuesto en las citadas leyes.

La prestación de servicios digitales a la ciudadanía exige que se haga de una manera segura. En relación a este aspecto de la prestación, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad, aprobado mediante Real Decreto 3/2010, de 8 de enero. La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios..

Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos. En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

A su vez el nuevo el nuevo 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 obliga a adoptar medidas técnicas para garantizar un nivel de seguridad adecuado en función de los posibles riesgos identificados.

El Servicio de Informática de la Consejería de Salud y Familias no dispone actualmente de infraestructura de seguridad apropiada que permita aplicar todas las medidas necesarias para ofrecer los servicios telemáticos de una manera segura, por ello LA CONSEJERÍA procede a plantear la renovación de su sistema de cortafuegos tanto en los SS.CC como en los centros directivos periféricos.

LA CONSEJERÍA, cuenta con un sistema de cortafuegos y seguridad perimetral actualmente basado en una conjunción de herramientas abiertas. Concretamente la gestión del Cortafuegos está basada en IPTables y la herramienta de gestión es FireWallBuilder. Además en torno al cortafuego se construye, como ya se ha indicado, todo un sistema de seguridad perimetral compuesto de IPS, captura y gestión de tráfico y otras herramientas …, todo ello aparece detallado en el ANEXO 1. SISTEMA DE CORTAFUEGOS EN SSCC, estas herramientas no tienen ya capacidades para aportar sinergias de gestión y seguridad al portfolio de aplicaciones actuales y las que se encuentran en desarrollo de cara al futuro.

Pero el proceso de adaptación a nuevas realidades tecnológicas que han posibilitado la atención y servicio a los ciudadanos ha hecho cada vez más complejo el ambiente tecnológico de LA CONSEJERÍA, existiendo incluso

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 5 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

actualmente un entorno de Hosting para determinados servicios prestados a las Delegaciones Territoriales de la Consejería, en adelante DD.TT, que cuenta con su propio sistema de cortafuegos basado en IPTables, como se describe en el ANEXO 2. SISTEMA DE CORTAFUEGOS EN HOSTING.

Además LA CONSEJERÍA ha dispuesto desde el año 2008 de sistemas de cortafuegos en las diversas DD.TT, para lo cual se han utilizado herramientas y tecnologías variadas. Todas las herramientas y tecnologías usadas para este fin se encuentran ya en franca obsolescencia, como puede verse en el ANEXO 3. SISTEMA DE CORTAFUEGOS EN DD.TT.

2 OBJETO DE LA CONTRATACIÓN

El objetivo de esta contratación es afrontar la sustitución del actual cortafuegos de los SS.CC de LA CONSEJERÍA así como de las DD.TT, para , como se ha indicado, conseguir que las nuevas aplicaciones desarrolladas o en desarrollo puedan implementarse con total funcionalidad y seguridad.

Para ello se pretende:

1 Mantener y mejorar las funcionalidades de los sistemas de seguridad actuales e incorporar otras nuevas más acordes al estado del arte de la tecnología de seguridad que directamente se vinculen como capa de control al software desarrollado en LA CONSEJERÍA.

2 Dotar al entorno de Hosting de LA CONSEJERÍA con un Cortafuegos diferenciado.

3 Dotar a las DDTT adscritas de sistemas perimetrales con las herramientas de seguridad exigidas en este pliego adaptadas a las necesidades derivadas del número de usuarios y ancho de banda. Además deberán proveer una capa de sencillez de gestión y seguridad extra que permita a los centros directivos periféricos el acceso a las aplicaciones desarrolladas por LA CONSEJERÍA.

4 Qué los nuevos sistemas de seguridad desplegados atiendan y cumplan los principios y requerimientos del nuevo 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. Este item es fundamental pues la articulación de los TRATAMIENTOS DE DATOS PERSONALES se producirá por estos nuevos aplicativos a desarrollar que exigen estas sinergias en cuanto a controles a implementar.

5 Que se puedan implantar de forma nativa los requerimientos en cuanto a controles que se definen en el Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad y que sean relativos al cortafuegos, aplicativos que presten servicios y a las diferentes infraestructuras desplegadas.

El objeto del presente expediente de contratación es el suministro, instalación, configuración y puesta en funcionamiento de la infraestructura indicada en el presente apartado, su parametrización y optimización , la migración de las políticas de seguridad vigentes en la infraestructura actual , y la ampliación de las medidas de seguridad a aplicar utilizando nuevas funcionalidades de la infraestructura a adquirir.

La solución de infraestructura estará compuesta por los siguientes subsistemas:

- Cluster de Cortafuegos para SSCC
- Cluster de Cortafuegos para el servicio de Hosting

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 6 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

- Cortafuegos para sedes de las Delegaciones Territoriales (DDTT) desde la que se ofrecen servicios a los ciudadanos.
- Infraestructura de red necesaria para su correcta conexión con la red existente en CSAFA

3 REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ENS

La nueva infraestructura debe adaptarse y cumplir los requerimientos que figuran en el nuevo Reglamento Europeo de Protección de Datos (R. EU 2016/679) y a los controles del R.D 3/2010 E.N.S que según la gradación de los sistemas se decidan aplicar en LA CONSEJERÍA.

3.1 Nuevo Reglamento Europeo de Protección de Datos (Reglamento (UE) 2016/679)

El nuevo Reglamento Europeo de Protección de Datos define un conjunto de principios técnicos y de acción que deben observarse en cualquier procesamiento de datos de carácter personal. Es fundamental que cualquier organización pueda demostrar que cumple estos principios que la habilitan a su realización.

La nueva infraestructura de seguridad a adquirir que supone el cortafuegos debe cumplir y habilitar para el cumplimiento de estos principios de forma nativa. Sin que exista una enumeración precisa y exacta de los controles a aplicar, el nuevo sistema de cortafuegos debe permitir la implantación de:

1. Mecanismos de Clasificación de Datos.
2. Controles de Gestión de Cambios en la configuración.
3. Separación de Roles en la ejecución de Tareas en la administración del dispositivo.
4. Control de Acceso.
5. Segmentación de Red.
6. Cifrado.
7. Mecanismos de Prevención de Fuga de Datos.
8. Prevención ante ataques DDOS.
9. Capacidad para monitorizar la actividad de los usuarios.
10. Gestión proactiva de las vulnerabilidades.
11. Previsión de escenarios de contingencias y recuperación ante desastres. Ver ANEXO 7. PLAN DE CONTINGENCIA

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 7 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

3.2 R.D 3/2010 Esquema Nacional de Seguridad (ENS)

En su anexo II el ENS describe una serie de controles que serán de aplicación a los sistemas según la gradación determinada en su análisis de riesgo correspondiente.

El nuevo sistema de cortafuegos debe permitir y facilitar la implantación de estos controles.

4 DESCRIPCIÓN DEL ENTORNO TECNOLÓGICO ACTUAL

El entorno tecnológico actual se esboza con la descripción de las tecnologías usadas en los cortafuegos a sustituir, así como los entornos de red a interconectar, en los ANEXOS 1, 2 y 3 de este pliego.

Si se requiriera más información técnica por motivos de seguridad y confidencialidad será suministrada en la modalidad de respuesta a cuestiones.

5 DESCRIPCIÓN DEL SUMINISTRO Y LOS SERVICIOS SOLICITADOS

Este proyecto de sustitución de la infraestructura de cortafuegos y herramientas de seguridad de LA CONSEJERÍA y de las DDTT se considerará como **LLAVE EN MANO**, es decir se deberá entregar completamente funcional atendiendo todos los requerimientos que se exponen en este pliego, corriendo el adjudicatario con todos los costes humanos y técnicos asociados.

El fabricante ofertado debe tener equipos cualificados para el cumplimiento del Esquema Nacional de Seguridad en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación del Centro Criptológico Nacional - Guia CCN-STIC 105 (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html) en el apartado “Familia: CORTAFUEGOS”.

Así mismo, el equipamiento ofertado debe implantarse siguiendo la configuración de seguridad de firewalls desarrollada por el Centro Criptológico Nacional para la tecnología propuesta.

La solución final es un conjunto de software y de hardware convenientemente relacionado entre sí, que constituya una solución integral que debe considerar los siguientes aspectos:

5.1 CARACTERÍSTICAS GENERALES

5.1.1 IDENTIFICACIÓN Y TRAZABILIDAD DE APLICACIONES

1 La herramienta debe permitir nativamente reconocer aplicaciones comerciales y habituales en Internet actualmente y las que puedan ir surgiendo durante el periodo de soporte solicitado, por ejemplo correos web, gestores de archivos, herramientas P2P (Cortafuegos Capa 7)

2 Se deben poder aplicar reglas a las aplicaciones reconocidas con la máxima granularidad posible o generar grupos para su tratamiento colectivo.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 8 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

3 Posibilidad de revisión y asignación de trazabilidad de aplicaciones a todos los puertos técnicos tanto TCP como UDP y no solamente en los reconocidos o habituales.

4 Acceso a detalles particulares como quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, etc.

5 Uso de la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red.

6 Existencia de un sistema de control de aplicaciones que puede basarse en diversos criterios que permita establecer los controles necesarios desde una sola consola gráfica de sencillo uso.

7 Se deben poder aplicar los mismos criterios anteriores a las aplicaciones desarrolladas por la Consejería de Salud.

8 Identificación de aplicaciones, no de puertos: Clasificación del tráfico para determinar la identidad de la aplicación, independientemente del protocolo, el cifrado o la táctica evasiva. Utilización de esa identidad como base de todas las políticas de seguridad.

9 El Firewall debe ser capaz de "clasificar" el tráfico entrante en base a la aplicación para después aplicar un "filtro" personalizado al consumo de esa aplicación (IPS, Antivirus, AntiSpyware, FileBlocking…) o determinar la aplicación.

Quedan especialmente excluidos aquellos firewalls que no permitan aplicar un perfil de seguridad diferente a aplicaciones que comparten atributos de red. Por ejemplo se excluirá un firewall que no pueda aplicar un perfil de "file blocking" diferente a las sesiones Facebook de las sesiones de Google-Drive.

10 Control del movimiento (upload/download) de ficheros.

11 Capacidad para inspeccionar tráfico https

5.1.2 IDENTIFICACIÓN DE USUARIOS

1 Integración con Microsoft Active Directory

2 Integración con LDAP.

3 Soporte de identificación de usuarios en entornos Windows Server 2008/2012/2016

4 Integración de usuarios y dispositivos en las políticas, no solo de direcciones IP: Creación y administración de políticas de seguridad basadas en la aplicación y en la identidad de los usuarios, independientemente del dispositivo o la ubicación

5.1.3 GESTIÓN Y ADMINISTRACIÓN

Se pretende disponer de una solución integrada de administración de seguridad que incluya políticas, registros, monitorización, correlación de eventos e informes que permita identificar fácilmente los riesgos de seguridad en la organización.

Deben aparecer las siguientes características:

1 Soporte de SNMP v2 y v3.

2 Exportación de logs vía FTP, SCP y TFTP.

3 Administración por GUI y CLI.

4 Creación de diferentes cuentas con diferentes niveles de acceso.

5 Auditoría de los cambios realizados en la configuración, comparación entre versiones de la configuración.

6 Bloqueo de la cuenta de administrador si se producen intentos fallidos reiterados.

7 Capacidad de crear diversos perfiles de administración.

5.1.4 SEGURIDAD

1 La política de seguridad tiene que poder agruparse en zonas correspondientes a las distintas VLANS que deben estar protegidas por el cortafuegos.

2 Debe permitir la segmentación virtual / compartimentación para poder cubrir los distintos ámbitos existentes y futuros que deben poder protegerse de forma aislada entre ellas (Front-end, Back-end, Red de Backup, red de Administración, etc.). Deberán aportarse al menos 10 licencias para dominios virtuales.

3 Tiene que contar con los mecanismos necesarios para el análisis de la política aplicada capaz de detectar solapamientos de reglas.

4 Diccionario de objetos completamente personalizable.

5 Debe soportar varios modos de funcionamiento y ser capaz de utilizarlos simultáneamente en diferentes interfaces:

5.1 Modo transparente para despliegue in-line.

5.2 Modo nivel 3/nivel 4.

5.3 Modo IDS.

6 Prevención de amenazas y detección de malware y exploits de vulnerabilidades sin incurrir en latencia no tolerables.

7 Tiempo de latencia con reglas integradas de firewalls no superior a 3 microsegundos.

8 Funcionamiento como IPS.

9 Definición de la identificación CVE o similar de las vulnerabilidades detectadas.

10 Se deben soportar múltiples sistemas de análisis de transferencia de ficheros y datos considerados como críticos basado en tipos de fichero y en análisis de transferencias realizado en tiempo real.

11 Bloqueo de ficheros por tipo, identificando por el tipo MIME y no basándose en la extensión del fichero.

12 Se valorará la posibilidad de realizar DLP (capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como de cadenas concretas)

13 Posibilidad de crear reglas dinámicas.

14 Posibilidad de monitorización y control de la navegación web sin penalizar el tiempo de respuesta ni la satisfacción del usuario.

15 Mecanismos que permita la toma de decisiones en tiempo real como por ejemplo permitir / denegar una URL, utilizando referencias a listas públicas reconocidas, alertas de seguridad de organismos públicos o decisiones de los técnicos de la Consejería.

16 No utilizar licenciamiento por usuarios (es decir, durante la duración de la contratación realizada del producto con su soporte solicitado puede incrementarse el número de usuarios), ni por caudal, ancho de banda o

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 10 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

cualquier otro concepto, como se explicita en el epígrafe 8 LICENCIAMIENTO Y GARANTÍA .

17 Aplicación de QoS por usuario, aplicación, zona: definición de ancho de banda garantizado, máximo y prioridad.

18 Descarga y aplicación automática de actualizaciones de las firmas antivirus, antispyware, base de datos de URLs, firmas IPS y de las nuevas aplicaciones identificadas.

19 Perfiles de administración parametrizables y personalizables.

5.1.5 SERVICIOS DE RED

Deben contemplarse los siguientes protocolos:

- Soporte de IEEE 802.1q VLAN tagging (capa 2, capa 3) en cada una de las interfaces.
- Control de flujo IEEE 802.3x
- Spanning Tree IEEE 802.1d.
- Spanning Tree de convergencia rápida IEEE 802.1w.
- Link Aggregation Control Protocol IEEE 802.3ad.
- Autentificación de red IEEE 802.1x.
- Prioridad QoS IEEE 802.1p, DSCP based Classification
- RMON
- Soporte de protocolos de routing: OSPF, RIPv2. Soporte de NAT y PAT.
- Site to site VPNs (IPSEC), SSL VPN
- Alta disponibilidad

5.1.6 OBTENCIÓN Y GESTIÓN DE INFORMES Y LOGS

La herramienta ha de reunir las siguientes funcionalidades:

1 Proveer de funcionalidad de análisis de logs y reporting con volumen de histórico de al menos 2 años sin penalización de la capacidad del sistema y con todas sus funcionalidades posibles. Funcionalidad de reenvío on-line de logs mediante syslog al concentrador de logs existente en LA CONSEJERÍA.

2 Herramienta de visualización de eventos de seguridad.

3 De ser necesario cualquier tipo de dispositivo o servidor para la gestión de Logs, correrá por cuenta del proveedor.

4 Capacidad para obtener informes de actividad por usuario.

5 Capacidad para agrupar informes en un único documento PDF.

6 Disponibilidad de mapa geográfico para identificar el origen y destino de los flujos y amenazas que entran y

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 11 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

salen de la red.

7 Informes sobre el ancho de banda utilizado por cada aplicación.

8 Capacidad de capturar tráfico en tiempo real y poder exportarlo a archivos (p.e pcap) para posterior análisis con herramientas tipo wireshark

A continuación se describen las características especificas de los equipos:

5.2 CLUSTER DE CORTAFUEGOS DE SSCC

El sistema de cortafuegos solicitado para los SS.CC de LA CONSEJERÍA debe constar, al menos, con dos nodos físicos que deben operar en modo "Alta Disponibilidad", que permita el despliegue en modo cluster activo-activo y en modo cluster activo-pasivo.

En cualquier caso cada uno de los nodos individualmente ha de reunir suficientes recursos tanto hardware como software para poder mantener activas todas las tareas que se configuren en modo cluster en caso de caída de uno de los nodos.

El sistema ofertado no puede tener ningún punto único de fallo. Todos los sistemas contemplados deberán disponer de componentes hardware activos redundantes con posibilidad de cambio en caliente (hotswap) de manera que se puedan sustituir sin interrupción del servicio.

Además de estos dos nodos que realizan la función de cortafuegos, cualquier otra funcionalidad exigida en este pliego y que pueda contemplarse separadamente, como hardware y/o software independiente, correrá a cargo del adjudicatario y se considerará incluida en la presente licitación, debiendo proveerlo el adjudicatorio. La provisión de una funcionalidad vía software supondrá que ha de entregarse el hardware suficientemente dimensionado para su ejecución. En cualquier caso el hardware suministrado por el proveedor pasará a ser propiedad de LA CONSEJERÍA.

5.2.1 CAPACIDAD Y RENDIMIENTO DE CADA NODO

Las siguientes especificaciones de rendimiento y capacidad deberán considerarse como requisitos **mínimos** que deberá cumplir el sistema de seguridad perimetral a suministrar.

Número de sesiones concurrentes	8.000.000
Número de sesiones nuevas por segundo	185.000
N.º de Politicas del Firewall	10.000
Rendimiento de Firewall (1518 byte UDP Packets))	36 Gbps.
Rendimiento IPS	10 Gbps.
Rendimiento NGFW	9,5 Gbps
Rendimiento Protección contra Amenazas	7 Gbps
Numero de túneles VPN IPSec cliente servidor	500

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 12 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

Numero de túneles VPN IPSec sede a sede	200
Usuarios concurrentes SSL-VPN	500

Ambos nodos presentarán una configuración idéntica entre ellos en lo que respecta a todas las capacidades y requerimientos hechos en este pliego.

5.2.2 OTRAS CARACTERÍSTICAS FÍSICAS

1 Al menos dos puertos 10 GE SFP+, con los transceivers necesarios para la solución.
2 Al menos 8 puertos Ethernet 10/100/1000 RJ45.
3 Se debe garantizar la no pérdida de logs ante escenarios de contingencia.
4 Puerto dedicado para gestión “out-of-band”.
5 Puerto de consola RJ45.
6 El fallo de los componentes de gestión (pe. Disco duro) no afectará al propio funcionamiento del cortafuegos.
7 Factor dimensiones: Encastrable en rack de 19”. Se debe incluir todo el material necesario para su encastrado.
8 Doble fuente de alimentación redundante y sustitución en caliente.

5.3 CORTAFUEGOS PARA EL SISTEMA DE ALMACENAMIENTO SERVICIO DE HOSTING

Se deberá proveer de un cluster más de cortafuegos dedicado exclusivamente para los servicios de hosting con las mismas características que el cluster de cortafuegos principal solicitado.y detallado en el epigrafe 5.2

Es requisito imprescindible para el despliegue que se mantenga el direccionamiento de los elementos de que componen el actual cortafuegos de hosting.

Se deberán trasladar todo el repertorio de políticas del actual cortafuegos a la nueva implementación, además se acordarán con la Dirección del Proyecto la puesta en funcionamiento de las diversas funcionalidades asociadas a la herramientas que se solicitan en este pliego.

5.4 INFRAESTRUCTURA DE RED

Es necesario para poder implementar la solución tanto del SSCC como del hosting el suministro de dos slots de 10 Gb

Tanto para el suministro del equipamiento de SSCC como el de Hosting, cada nodo se conectará mediante una agregación (LACP o similar) de dos enlaces 10 GE al switch de CORE (formado por dos equipos HP 10508 con conexión IRF entre ambos). Para ello se deberá suministrar el siguiente hardware para dicho switch:

- 2 módulos "HPE 10500 16p 1/10GbE SFP+ SF Mod (JH193A)"

JOSE DANIEL SOTO ALBA | 09/01/2020 | PÁGINA 13 / 38
VERIFICACIÓN | NJyGwRjA4DDQxOy2u52o4X8gCEFMAt | https://ws050.juntadeandalucia.es/verificarFirma

- 8 transceiver "HPE X130 10G SFP+ LC SR Transceiver (JD092B)"
- Cualquier medio físico para la conexión entre cada nodo del FW y el switch CORE, como latiguillos o cableado de fibra necesario, etc.

Además se deberá realizar las tareas de instalación y configuración de los mismos, incluyendo cualquier actualización software del Switch CORE que fuera necesaria sin afectar al servicio productivo. Ésta tareas deberán incluirse en el Plan de Instalación y Migración del sistema, y deberán realizarse por personal acreditado por el fabricante.

5.5 SISTEMAS DE CORTAFUEGOS Y HERRAMIENTAS DE SEGURIDAD PARA LAS DD.TT

Dada la diversidad de las distintas DD.TT y centros periféricos adscritos a LA CONSEJERÍA se ha escogido para la solución una gradación a la hora de selección de la herramienta de cortafuegos a implementarse en cada uno de ellos, si bien en todos los casos se debe garantizar la posibilidad de gestión remota y aplicación de políticas desde una única consola gráfica centralizada ubicada en el Cortafuegos de los SS.CC de LA CONSEJERÍA.

En el ANEXO 3. SISTEMA DE CORTAFUEGOS EN DD.TT se detallan los diversos tipos de centros periféricos a atender, con los requerimientos de ancho de banda y demás requisitos básicos especificados. La empresa adjudicataria deberá proporcionar la infraestructura necesaria para atender al menos los siguientes ítems:

1. Como utilidad fundamental, permitir la administración centralizada del dispositivo de los SS.CC de LA CONSEJERÍA y también delegada del mismo.
2. Gestión de cortafuegos simple y sencilla a nivel de aplicación, mediante la misma interfaz gráfica que la usada en LA CONSEJERÍA.
3. Funcionamiento como IPS y Cortafuegos (NGFW Y THREAT PROTECTION).
4. Gestión de Logs local y consolidación de logs remota en LA CONSEJERÍA.
5. Posibilidad de establecer varias Vlanes físicas.
6. Capacidad de realizar QoS.
7. Obtención de gráficos e informes mediante Sflow o similar. Estadísticas de tráfico y su tratamiento de manera centralizada (off-line)

Se habrán de suministrar (con el montaje en las sedes tipo 1) incluyendo la migración de su política y también bajo la modalidad LLAVE EN MANO los dispositivos enumerados en el ANEXO 3. SISTEMA DE CORTAFUEGOS EN DD.TT.

Es importante tener en cuenta que la implantación y despliegue siempre será presencial en las sedes de Tipo 1. Para el resto de sedes la configuración se realizará en SSCC y será enviado por cuenta del adjudicatario a la sede correspondiente. El personal de la sede realizará su implantación siguiendo las directrices de la empresa adjudicataria.

El régimen de despliegue y montaje es el solicitado en 5.8.2 LA INSTALACIÓN DEL HARDWARE Y SOFTWARE OFERTADO.

5.6 INTEROPERABILIDAD TECNOLÓGICA

Partiendo de que el suministro solicitado en el presente pliego por su naturaleza técnica no va a tener efecto en el marco de interoperabilidad, de preverse tal eventualidad por parte de las empresas licitantes, las ofertas que se presenten deben ser conformes a la normativa que sobre el Marco de Interoperabilidad digital haya dictado la Junta de Andalucía y por la que se pretende la normalización de los formatos, protocolos e interfaces que permitan garantizar el principio de neutralidad tecnológica, la interoperabilidad de los servicios y sistemas de información inter-administraciones, así como la preservación del conocimiento general y la gestión eficaz y eficiente del uso de las TIC.

http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/19

5.6.1 ADAPTACIÓN AL ESQUEMA NACIONAL DE INTEROPERABILIDAD

En definitiva la solución propuesta en cada oferta deberá estar adaptada al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5.7 PLAN DE DESPLIEGUE

El adjudicatario deberá presentar un PLAN PRELIMINIAR DE DESPLIEGUE basándose en la información que se aporta en este pliego y en sus anexos donde se detalle todo el proceso a realizar, así como la ingeniería y recursos necesarios para su ejecución.

Obviamente se requieren planes preliminares de despliegue individualizados para los distintos cortafuegos de las sedes de LA CONSEJERIA, no obstante se podrá plantear un Plan Modelo que sea aplicable de forma estándar a las diversas sedes provinciales de la Consejería.

Todo el plan deberá partir de los siguientes preceptos:

a) Mantener el direccionamiento actual.

b) Mantener la infraestructura actual de cortafuegos asociado al plan de contingencia y con fácil vuelta atrás. Ver ANEXO 7. PLAN DE CONTINGENCIA

c) Garantizar el mantenimiento de los servicios prestados en el momento previo a la migración.

d) Traslado de las políticas vigentes.

Y deberá contener al menos:

1 Esquema de la solución propuesta tanto a nivel físico (hardware y conectividad) como funcional.

2 Exposición de la ingeniería a realizar.

3 Detalle específico de los trabajos de estudio y migración de reglas a realizar en cada uno de los cortafuegos a sustituir.

4 Previsión del tiempo y recursos humanos y técnicos a invertir por parte de la empresa adjudicataria.

5 Previsión del tiempo y recursos humanos y técnicos a aportar por parte de LA CONSEJERÍA.

6 Cronograma detallado de todas las instalaciones a realizar tanto en SS.CC como en las DD.TT.

7 Planes de pruebas a realizar.

8 Planes de contingencia a poner en marcha ante posibles fallos. Este plan deberá contener las medidas a seguir para posibilitar el “paso a atrás” en el despliegue, retornando a las infraestructuras y funcionalidades anteriores. Ver ANEXO 7. PLAN DE CONTINGENCIA

9 En cualquier caso en este plan preliminar de despliegue deberá de adaptarse a los requerimientos respecto a plazos de aprovisionamiento y ejecución que se establecen en los puntos 7 PLAZOS, TASACION Y FACTURACION DEL PROYECTO e 5.8 INSTALACIÓN Y CONFIGURACIÓN.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 15 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

Una vez realizada la adjudicación y firma de contrato este plan preliminar de despliegue se perfeccionará en un PLAN DEFINITIVO de despliegue en el plazo de un mes desde la firma del contrato que será el que se seguirá durante todo el suministro y que deberá contar con la aprobación del Director del Proyecto por parte de LA CONSEJERÍA. Todo el procedimiento se realizará conforme a las mejores prácticas de ITIL y se gestionará con las herramientas propias de LA CONSEJERÍA para la gestión de tiques (GESTIC). para ello se atenderá la metodología, nomenclatura y mecanismos de puestas en producción que LA CONSEJERÍA mantiene de forma efectiva., al igual que el mantenimiento de la información derivada se realizará en su Wiki.

Toda la información generada que no sea directamente registrada en la wiki lo será en formato documental abierto ODF y utilizando LibreOffice y sus diversas herramientas.

Para cualquier personal del equipo anteriormente citado o el Jefe de Proyecto, así como el personal que se destaque para cumplir los servicios que se solicitan en este pliego podrá ser solicitada su sustitución por parte de LA CONSEJERÍA, con un aviso previo de 15 días naturales.

5.8 INSTALACIÓN Y CONFIGURACIÓN

Serán también objeto del presente contrato todos los servicios necesarios relacionados con la instalación y puesta en marcha de los equipos.

Como ya se ha indicado esta contratación se ha definido como **"Llave en Mano"** con lo cual se debe producir la entrega completamente funcional de la infraestructura de cortafuegos descrita, es decir, todas las tareas de instalación, configuración, parametrización se entienden incluidas y deberán producirse de común acuerdo con la Dirección del Proyecto por parte de LA CONSEJERÍA.

El suministrador garantizará la plena operatividad de todo el hardware y el software ofertado, así como su integración con la infraestructura existente.

5.8.1 LA INGENIERÍA DE PUESTA EN FUNCIONAMIENTO Y ARRANQUE

Para la puesta en marcha de los equipos, el adjudicatario se responsabilizará de la instalación de los sistemas y sus elementos, y asegurará la plena operatividad de los mismos una vez instalados. Para ello se considerarán incluidos en la oferta todos los dispositivos, conectores, latiguillos, accesorios y otros elementos hardware o software que fueran requeridos (incluidos los adaptadores Gbic necesarios).

Todos los productos, hardware y software, deberán suministrarse con manuales originales de operación y referencia y toda la documentación necesaria, preferiblemente en castellano, o en su defecto en inglés. Se deberá entregar al menos un juego de manuales por cada sistema o producto suministrado, además de sus versiones digitales.

La empresa adjudicataria deberá trabajar coordinadamente con el Director del Proyecto y el equipo designado por LA CONSEJERÍA para:

1 Planificar y diseñar la arquitectura definitiva de la solución, incorporando nuevo equipamiento.

2 Realización de las tareas de instalación y configuración.

2.1 Instalará y configurará el nuevo equipamiento relativo a:

2.1.1 Conectividad: Instalación y configuración de Switches.

2.1.2 Creación de reglas en los Firewalls.

2.1.3 Instalación y configuración.

2.1.4 Pondrá en marcha las funcionalidades incorporadas.

3 Definición y Ejecución de pruebas y validación del funcionamiento. Ver ANEXO 4. PLAN DE PRUEBAS

5.8.2 LA INSTALACIÓN DEL HARDWARE Y SOFTWARE OFERTADO

La instalación del hardware y software ofertado se realizará dentro de los plazos indicados en este pliego tanto para SS.CC como para las DD.TT y sedes territoriales que se incluyan. Tanto los componentes descritos y ofertados por la empresa adjudicataria como los que puedan descubrirse como necesarios correrán por su cuenta.

La instalación se realizará conforme a los plazos (ver apartado 7 PLAZOS, TASACION Y FACTURACION DEL PROYECTO determinados en este Pliego). Concretamente y como un hito crítico considerado por la Dirección del Proyecto, tras la puesta en marcha del cluster de cortafuegos de SSCC deberá transcurrir al menos cinco (5) días hábiles de funcionamiento de la infraestructura en los que el mismo personal que ha realizado la instalación y despliegue por parte de la empresa adjudicataria mantenga su presencia en los SS.CC de LA CONSEJERÍA, tras los cuales comenzará la prestación del servicio de administración de la plataforma solicitado en este pliego.

Para el caso del cortafuegos de hosting se considerará como necesarios cinco (5) días hábiles de funcionamiento.

Para las soluciones desplegadas en las DD.TT se deberá aplicar un periodo de comprobación como el descrito arriba con las siguientes características

Sedes Tipo /Dispositivo Tipo	Número de días de comprobación.
Tipo 1	2 días tras la instalación
Tipo 2	Las 3 primeras sedes del tipo: 2 día tras la instalación.
	Resto de sedes grupo mismo día.
Tipo 3 y 4	Mismo día.

5.8.3 MIGRACIÓN DE LA POLÍTICA ACTUAL

Reconociéndose que la migración de las actuales políticas y reglas de cortafuegos (que se encuentran definidas en las tecnologías ya descritas en la introducción de este pliego), se exigirá un minucioso trabajo previo que debe constar de:

1. Estudio de la política y repertorio de reglas actuales.
2. Estudio y análisis del tráfico real.
3. Simplificación y mejora de la la política actual y reglas definidas, cumpliendo los niveles de seguridad actualmente aplicados.
4. Migración de la política y reglas actualmente aplicadas.

5.8.4 MONITORIZACION DE LA INFRAESTRUCTURA

Además de la configuración de las herramientas de monitorización disponibles en la infraestructura, se deben crear los scripts o monitores que sean necesarios para integrar una monitorización básica en NAGIOS (al menos con el mismo nivel de granularidad con el que se monitoriza la infraestructura de seguridad actual), de tal forma que el servicio de soporte a Sistemas (24x7) de la Consejería pueda detectar situaciones anómalas en el funcionamiento de la infraestructura.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 17 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

5.8.5 TRANSFERENCIA DEL CONOCIMIENTO

Es necesario impartir formación equivalente al programa de certificacion básica del fabricante del cortafuegos.

Se incluirá en la oferta un plan de formación que contendrá, al menos:

1. Tareas de capacitación técnica especializada sobre las tecnologías y funcionalidades incorporadas por el nuevo equipamiento en el proyecto.
2. Operatoria, uso y gestión de todos los elementos y funcionalidades incorporados a la infraestructura de Cortafuegos desplegada según este pliego (para los distintos perfiles que participen en la operación y administración de la plataforma).
3. Conocimientos necesarios para la adquisición de una certificación de nivel básico dentro del sistema de certificaciones del fabricante del cortafuegos y que habilite el desempeño normal del mismo.

Se incluirá dentro de la formación establecidas las jornadas formativas necesarias para el personal encargado de administrar los cortafuegos en las distintas sedes seleccionadas para su instalación.

Esta formación será mediante los sistemas de videoconferencia y conexión remota que provea LA CONSEJERÍA.

Durante la ejecución del contrato se realizarán periódicamente actividades adicionales de transferencia de conocimiento que capaciten a los técnicos de la Consejería.

5.9 SERVICIO DE ADMINISTRACIÓN DE LA PLATAFORMA

El servicio de administración de la plataforma comenzará tan pronto como se haya validado la puesta en funcionamiento del cluster de cortafuegos de SSCC, una vez transcurrido al menos cinco (5) días hábiles después de dicha fecha. Se prolongará hasta la finalización del contrato.

Es un servicio que se solapará parcialmente en el tiempo con el servicio de Instalación y Configuración de los cortafuegos de Hosting y DDTT. Los trabajos de despliegue de los Cortafuegos de Hosting y DD.TT no se computarán como trabajo propio de este servicio.

El propósito de este servicio es mantener completamente operativa la infraestructura a la vez que se van incorporando las nuevas capacidades de la infraestructura adquirida.

Para ello se debe colaborar con el grupo de soporte a Sistemas de la Consejería, que se encargará de realizar la tareas que se estimen oportunas fuera del horario de prestación del servicio (en horario 24x7). Por ello es necesario procedimentar y documentar todos los trabajos de operación y administración de la plataforma, así como realizar las sesiones necesarias de transferencia de conocimientos que garanticen que el trabajo se ejecute de una manera óptima (tanto al primer nivel de soporte como al segundo nivel especializado de soporte).

Se realizarán entre otros los siguientes trabajos:

- Operación y administración de la infraestructura
- Automatización de trabajos habituales
- Monitorización del estado (del servicio prestado por la plataforma y del riesgo de seguridad existente, etc.)
- Integración con las herramientas que actualmente se usan en LA CONSEJERIA para que aporten una solución integral (NAGIOS).

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 18 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

- Elaboración de informes tipo y de los procedimientos de creación de nuevos informes
- Elaboración de procedimientos a utilizar durante la operación y administración del sistema
  - Procedimientos de trabajos diarios parametrizables para que sean realizados de una forma más sencilla.
  - Procedimiento para optimizar y limpiar reglas
  - Procedimientos para poder crear alertas que considere LA CONSEJERÍA en la herramienta de la CONSEJERÏA
  - Procedimientos para la configuración de nuevas funcionalidades
- Proyectos de mejoras y uso de todas las funcionalidades disponibles en la plataforma.
- Sesiones de transferencia de conocimiento

5.9.1 CONDICIONES DE PRESTACION DEL SERVICIO

El servicio se prestará preferentemente de forma presencial, complementado con un servicio en modo remoto. El equipo de trabajo realizará sus tareas de forma habitual, en la sede de los servicios centrales de la Consejería de Salud y Familias en Sevilla, en el lugar de ubicación del Centro de Proceso de Datos.

El horario habitual de prestación del servicio será el comprendido de lunes a viernes entre las 7:30 horas y las 14:30 horas, y al menos cinco horas adicionales semanales durante la jornada de tardes en horario de 15:00 a 20:00.

Todos los trabajos deberán realizarse en la medida de lo posible sin impacto sobre el entorno de producción. De manera puntual se podrán planificar actuaciones que se realizarán fuera del horario arriba indicado (incluyendo de forma puntual noches, sábados, domingos y festivos) cuando la actuación no se pueda realizar sin producir pérdidas de servicio en elementos críticos de la infraestructura (cluster de cortafuegos de SSCC).

Se valorará que se amplíe la disponibilidad del servicio de administración de la plataforma, de tal forma que se puedan atender y resolver las incidencias criticas que se produzcan fuera del horario de soporte (en horario 24x7), aquellas incidencias que no puedan resolver los técnicos de guardia de la Consejería con los procedimientos de actuación que se hallan definido en el ámbito de este servicio.

El horario del servicio prestado de manera presencial podrá verse afectado por las circunstancias y necesidades en cada momento de los proyectos y sistemas de información de la Consejería de Salud y Familias objeto de la administración y soporte del presente pliego.

Es responsabilidad de la empresa adjudicataria y de sus delegados impartir todas las órdenes, criterios de realización del trabajo y directrices a sus trabajadores siendo la Administración Pública de todo ajena a estas relaciones laborales y absteniéndose, en todo caso, de incidir en las mismas. Corresponde asimismo a la empresa contratista de forma exclusiva, la vigilancia del horario de trabajo de los trabajadores, las posibles licencias horarias o permisos o cualquier otra manifestación de las facultades del empleador. No obstante, es responsabilidad exclusiva del adjudicatario, en la forma establecida en los pliegos, asegurar que el servicio quede convenientemente cubierto.

5.9.2 COMPOSICION DEL EQUIPO

El equipo de trabajo debe estar formado por al menos un técnico que haya participado de manera activa en el despliegue del cluster de cortafuegos de SSCC. Este técnico ofrecerá soporte presencial en las instalaciones de la Consejería.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 19 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

Dicho técnico no podrá ser sustituido por la empresa adjudicataria durante la ejecución del contrato, para así asegurar el buen funcionamiento de los trabajos, a menos que el Director de Proyecto de la Consejería lo estime conveniente.

5.9.3 TASACION DEL SERVICIO

Este servicio se realizará por al menos 2.250 horas de Técnico.

El precio de la hora base de servicio se calculará utilizando la siguiente formula:

PHBS = IADJ * PESO / (HES + IHO)

Siendo:

PHBS = Precio de Hora Base Servicio sin IVA

PESO = Peso del servicio de administración en el total del contrato = 0,0825

IADJ = Importe de Adjudicación sin IVA

HES = Horas totales del Servicio de Administración = 2250

IHO = Incremento de Horas Ofertadas

Ejemplo:

Si el importe de adjudicación es de 590.000 y se ofertan 50 horas adicionales el precio de la hora seria:

PBHS = 590.000 * 0,0825 / (2250 + 50) = 21,16

6 CONDICIONES GENERALES DE EJECUCIÓN Y SUMINISTRO

6.1 LUGAR DE EJECUCIÓN DE LOS TRABAJOS

Los lugares de ejecución de los trabajos son las sedes de la Consejería de Salud y Familias, que se relatan en el ANEXO 5. SEDES Y LUGARES DE REALIZACIÓN DEL TRABAJO. Los trabajos de instalación y configuración se realizarán presencialmente en la sede de SSCC y en sedes tipo1 de la DDTT. La administración se realizará centralizadamente desde la sede de SSCC.

6.2 PROCEDIMIENTOS DE TRABAJO

Se estará a lo dispuesto en los procedimientos, buenas practicas y modelos de trabajo que LA CONSEJERIA tiene establecido en su operatoria diaria.

La gestión de los cambios que entrañe la puesta en producción de las nuevas infraestructuras de cortafuegos y los proyectos de los que procedan se articularán mediante el sistema de tiques que tiene LA CONSEJERÍA.

Respecto a la documentación generada, se efectuará en los formatos y mediante los procedimientos implementados en LA CONSEJERÍA.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 20 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

6.3 MEDIOS MATERIALES Y HUMANOS

Por parte del adjudicatario se deberán proveer todos los medios técnicos y humanos necesarios y descritos en este pliego y cualquier otro que pueda derivarse del proceso de despliegue y administración de la plataforma.

Es importante tener en cuenta que la implantación y despliegue siempre será presencial tanto en los SS.CC de LA CONSEJERÍA como en las sedes de Tipo 1. Para el resto de organismos la configuración se realizará en SSCC y será enviado por cuenta del adjudicatario a la sede correspondiente. El personal de la sede realizará su implantación siguiendo las directrices de la empresa adjudicataria.

Correrá por cuenta del adjudicatario los desplazamientos, portes y envíos así como cualquier coste derivado de estos despliegues que deberán realizarse, al menos, con los plazos y cautelas de revisión que se expongan en este pliego, ver el apartado 7 PLAZOS, TASACION Y FACTURACION DEL PROYECTO

En la entrega de los bultos mediante los que se provea la solución propuesta por el adjudicatario, deberá estar presente el responsable de la empresa adjudicataria para la validación de la entrega del material. La recepción se realizará conjuntamente con la persona designada por el Director del Proyecto por parte de LA CONSEJERÍA.

6.4 INSTALACIÓN Y PUESTA EN MARCHA

El suministrador incluirá todos los dispositivos, adaptadores, cableado y cualquier accesorio hardware y/o software para el perfecto funcionamiento del sistema descrito. Así mismo, correrán por su cuenta todos los trabajos y costes derivados del transporte, descarga, traslado del material a su ubicación definitiva en cada sede, desembalaje, instalación, configuración, puesta en funcionamiento a plena operatividad del conjunto ofertado, y retirada del material de embalaje.

Es de especial atención que será el adjudicatario quien aportará cualquier adaptador, cableado o cualquier otro dispositivo necesario para que el nuevo sistema se integre completa y funcionalmente en la red de LA CONSEJERÍA.

6.5 PLANES DE CONTINGENCIA Y GARANTÍA DE CONTINUIDAD DEL SERVICIO

Como ya se ha indicado en el punto referente 5.7 PLAN DE DESPLIEGUE, el adjudicatario deberá aportar un plan de despliegue que contenga un plan de contingencia (ver ANEXO 7. PLAN DE CONTINGENCIA) que permita la recuperación del servicio ante errores durante todo el contrato incluyendo la garantía y problemas tras la migración.

6.6 PROCEDIMIENTO DE ETIQUETADO E INVENTARIADO DE BIENES

Todos los bienes suministrados mediante el presente expediente requieren ser etiquetados tanto a nivel físico como lógico 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 articulo 14, asi como la Orden de 23 de Octubre de 2012 por la que se desarrollan determinados aspectos 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 debe 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 suministradora deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes anexado al presente pliego, y tomar 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

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 21 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

etiqueta en los términos que describe el procedimiento de inventariado.

6.7 MEDIDAS DE INFORMACIÓN Y PUBLICIDAD (fondos FEDER)

Para el cumplimiento de la normativa comunitaria en materia de publicidad de las actuaciones cofinanciadas con fondos FEDER, el adjudicatario deberá realizar un serigrafiado informativo de los bienes suministrados. Dicho serigrafiado deberá realizarse en un lugar que quede visible tras la instalación del suministro y en caso de que no fuera posible para cualquiera de los bienes deberán realizarse carteles informativos. El diseño y la producción de las serigrafías y/o carteles informativos serán realizados por el adjudicatario. En el caso de requerirse carteles, el servicio incluirá el transporte de los mismos a los centros destinatarios del equipamiento. Las características serán las siguientes:

• Contenido: Emblema de la Unión Europea, acompañado de los logotipos institucionales y referencias. Para la validación de artes finales, se requerirá la entrega de una muestra por proyecto en la sede de la Entidad.

• En el caso de carteles:

◦ Dimensiones: 0,25 x 0,25 m

◦ Material: Impreso en hexacromia sobre papel blanco de 170 gr. con laminado antirreflex en su cara anterior montado sobre foam 10 mm, perfilado en aluminio plata.

• En el caso de serigrafías, las dimensiones serán aquellas que permitan su correcta visualización en función de la instalación física del bien, a criterio del Director de Proyecto.

Así mismo toda la documentación e informes generados durante la ejecución del expediente deberá ir identificada con el emblema de la Unión Europea acompañado de los logotipos institucionales.

6.8 CONFIDENCIALIDAD DE LA INFORMACIÓN

La información a la que tenga acceso la empresa adjudicataria como consecuencia de los trabajos objeto del presente contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de la Junta de Andalucía. La empresa adjudicataria, en cumplimiento de la “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.) únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones del LA CONSEJERÍA, y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en sudesarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

Se atenderá también a la normativa interna de LA CONSEJERIA en materia de Seguridad TIC.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccncert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.

Además teniendo en cuenta que toda la información técnica tratada tiene carácter de sensible por su naturaleza, se le aplicarán las mismas guardas y cauciones, operando la obligatoriedad de petición de permiso a LA CONSEJERÍA para cualquier uso o difusión, comercial o de cualquier tipo en la que se haga referencia a dichos trabajos.

6.9 PROPIEDAD INTELECTUAL DE LOS TRABAJOS

Todos los documentos y resultados de los trabajos realizados y en particular, la propiedad intelectual de las modificaciones y/o mejoras que se introduzcan o realicen en el despliegue de la solución y su integración con el entorno tecnológico de cada sede, especialmente de toda la documentación que se genere, serán propiedad de LA

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 22 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

CONSEJERÍA, pudiendo reproducirse o divulgarse por ésta. La empresa adjudicataria podrá hacer referencia a la realización de dichos trabajos siempre que cuente para ello con la autorización expresa de LA CONSEJERÍA.

7 PLAZOS, TASACION Y FACTURACION DEL PROYECTO

7.1 PLAZOS DE SUMINISTRO Y PUESTA EN FUNCIONAMIENTO

El cuadro indicativo de todos los plazos exigidos es el siguiente:

Concepto.	Plazo según tipo sede	Observaciones.
Plazo de entrega Plan de Despliegue definitivo para SS.CC y DD.TT.	Un (1) Mes desde la firma del contrato.	
Plazo de entrega de los Cortafuegos de SS.CC y de los cortafuegos de de Hosting de la Consejería de Salud y Familias.	Un (1) Mes desde la firma del contrato.	
Plazo de entrega de los dispositivos de las DD.TT.	Dos (2) Meses desde la firma del contrato.	Por causas de fuerza mayor o interés de la Consejería se podrán demorar estas entregas, según marque el Director del Proyecto.
Plazo de instalación, migración y puesta en funcionamiento del Cortafuegos de SS.CC y de Hosting.	Tres (3) Meses desde la entrega.	
Periodo de prueba y garantía de la infraestructura de cortafuegos de SSCC con soporte presencial.	Al menos una (1) semana de 5 días laborables tras la instalación.	Este periodo de tiempo está vinculado a la resolución del cambio o marcha atrás del mismo. Por lo tanto será iterativo y obligado para cada subida a producción en esta fase.
Periodo de prueba y garantía de la infraestructura de cortafuegos de Hosting con soporte presencial.	Al menos una (1) semana de 5 días laborables tras la instalación.	
Plazo de instalación, migración y puesta en funcionamiento de los Cortafuegos de las DD.TT.	Nueve (9) meses desde la entrega.	
Periodo de prueba y garantía de infraestructura de los cortafuegos de las DD.TT.	Tipo 1: Dos (2) días tras la instalación.	
	Tipo 2: Las Tres (3) primeras sedes dos(2) dias y el resto mismo dia tras la instalación.	
	Tipo 3 y 4: Mismo dia tras la instalación.	
Inicio de la Garantía Oficial del producto.	Tras el periodo de prueba de la infraestructura completa (Cortafuegos SCCC + Hosting) y transcurrido su plazo de prueba estipulado. Las garantías serán, como se exige en este pliego de al menos cinco (5) años.	

En cualquier caso por indicación del Director del Proyecto y por coincidencia con periodos de vacaciones o acúmulo de

JOSE DANIEL SOTO ALBA | 09/01/2020 | PÁGINA 23 / 38
VERIFICACIÓN | NJyGwRjA4DDQxOy2u52o4X8gCEFMAt | https://ws050.juntadeandalucia.es/verificarFirma

trabajo periódico en LA CONSEJERÍA que imposibiliten su ejecución podrán retrasarse o ampliarse los plazos indicados, sin que suponga penalización para el adjudicatario.

7.2 TASACION Y FACTURACION DEL PROYECTO

A efectos de facturación, se establece la tasación del proyecto tal y como se define en la siguiente tabla:

Fase	Hito	Tasación sobre Importe Adjudicación	Número Sedes	Porcentaje Total sobre Importe Adjudicación
Instalación y Configuración	Suministro del Hardware	50%		50%
Instalación y Configuración	Instalación y Configuración del cluster de cortafuegos de SSCC	5,95%	1	5,95%
Instalación y Configuración	Instalación y Configuración de cluster de cortafuegos de Hosting	5%	1	5%
Instalación y Configuración	Instalación y Configuración de cluster de cortafuegos Sede Tipo A,B,C	2%	13	26%
Instalación y Configuración	Instalación y Configuración de Sede Tipo D	0,6%	8	4,8%
Servicio de Administración		8,25%		8,25%

8 LICENCIAMIENTO Y GARANTÍA

8.1 CARACTERISTICAS GENERALES

Todos los elementos tanto hardware como software que componen la solución en todos sus niveles mantendrán una garantía COMPLETA Y OFICIAL del FABRICANTE / FABRICANTES así como las ACTUALIZACIONES COMPLETAS durante al menos 5 años.

La petición de licencias para los diversos productos se justifica por las funcionalidades específicas que tiene los elementos componentes de la solución y la imposibilidad de conseguir un nivel equivalente usando herramientas exclusivamente abiertas.

Se considerarán cubiertas cualquier actualización tanto de hardware, software, firmas de virus o cualquier otro malware, microcódigos, firmware o cualquier otra que pueda aparecer durante el tiempo de vigencia de la garantía.

La garantía será siempre en el local de instalación de la solución (debiendo efectuarse las intervenciones, según el caso, en cualquiera de los centros que forman el alcance de este proyecto) y dispensada por un técnico con las convenientes certificaciones, especialmente cualquier actualización de software o hardware que pueda cuestionar el funcionamiento del Cortafuegos o cualquiera de sus sistemas satélites deberá de ser realizada de forma presencial por técnicos que representen la GARANTÍA OFICIAL DEL FABRICANTE.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 24 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

El adjudicatario debe poner a disposición de LA CONSEJERÍA un servicio de atención 24x7 que permita reportar las incidencias que se produzcan, **con un tiempo máximo de respuesta** inferior a 4 horas y un tiempo máximo de resolución del siguiente día laborable (NBD), según calendario laboral de la Junta de Andalucía. A estos efectos, se debe de considerar horario laboral el comprendido de lunes a viernes de 8:00 a 20:00 horas.

Estas asistencias o actuaciones no imputarán contra la bolsa horaria anual solicitada en este pliego.

De la misma manera se entenderán incluidas en las mismas condiciones expresadas en este punto las licencias asociadas a cualquier software propio del fabricante o de terceros incluidos en la solución que sean necesarias.

No se utilizará ningún licenciamiento por usuarios, tanto para productos software como hardware (es decir puede incrementarse el número de usuarios), por caudal, ancho de banda, memoria consumida o cualquier otro concepto; es decir una vez desplegadas y operativa las soluciones solicitadas, cualquier funcionalidad requerida en este pliego o que se deriva como necesidad de alguna funcionalidad pedida podrán usarse sin ninguna limitación.

Esta carencia de limitación de licenciamiento por cualquier concepto es extensible a cualquier actualización tanto de hardware como de software que haya que realizar al dispositivo.

La garantía del hardware debe incluir el reemplazo y/o sustitución por cualquier avería que pueda producirse sin costo alguno para LA CONSEJERÍA. Incluirá la totalidad de las prestaciones humanas y materiales requeridas para la subsanación de los defectos observados en las instalaciones de los sistemas objeto de este procedimiento y, eventualmente, derivados de la incorrecta prestación de los servicios contratados.

Todos los dispositivos contarán con garantía de sustitución y reposición a nuevo si se solicita por parte de LA CONSEJERIA si estuviese convientemente justificado.

En cualquier caso, en las ofertas, se deberá describir con detalle las caracteristicas del soporte técnico de la empresa adjudicataria: personal técnico, medios de contacto, horario de atención y acuerdos de nivel de servicio acordados.

Todos los trabajos deberán realizarse obligatoriamente sin impacto sobre el entorno de producción: si alguna tarea no pudiera realizarse de esta manera, deberá especificarse en la planificación y realizarse el trabajo íntegramente sin coste adicional, en el horario que para ello establezca la Consejería.

El fabricante deberá de ser el que proporcione de forma directa la posible ejecución de las anteriores garantías con las condiciones antedichas. Asímismo, garantizará la disponibilidad de piezas, al menos, durante los 5 años siguientes a la adjudicación. Durante el mismo periodo de garantía deberá asegurarse además la compatibilidad del hardware con nuevas versiones o revisiones de firmware.
Asímismo, para TODAS las licencias software que deban ser suministradas, se incluirá en sus condiciones de licenciamiento la propiedad o uso por tiempo ilimitado

8.2 ATENCION REMOTA DE CUESTIONES, DUDAS Y CASOS DE SOPORTE

Se atenderá, por parte del FABRICANTE DE LA SOLUCIÓN y en su caso del adjudicatario sin limitación alguna de forma telemática o telefónica, preferentemente en español, las dudas y cuestiones planteadas por el equipo técnico de LA CONSEJERÍA referentes a estos productos.

Además debe garantizarse el acceso por las mismas vías y en las mismas condiciones al servicio técnico de soporte del propio fabricante.

El horario definido para este soporte será de lunes a domingo de 8.00 a 20.00, incluyendo festivos, durante toda la vida del contrato y la garantía.

Además se contará con una línea ilimitada de consultas vía teléfono y/o correo electrónico que mantendrá el adjudicatario de la presente contratación como se ha indicado en el epígrafe.

8.3 BOLSA HORARIA

Se contará durante el periodo de garantía con una bolsa horaria de al menos **40 horas anuales** que tendrá carácter de presencial y ejecutado por técnicos certificados por el fabricante, a petición de la Dirección del Proyecto de LA CONSEJERÍA

8.4 CASO ESPECIAL DE FIRMWARE Y ACTUALIZACIONES

Las actualizaciones que requieran la instalación de un Firmware, Microcódigo o cualquier otra actualización de bajo nivel tanto de Hardware como de Software se realizará por parte de la empresa adjudicataria **PRESENCIALMENTE en las sedes de Tipo 1 y de forma remota en el resto de las sedes, durante toda la vigencia del contrato y durante el periodo de la garantia.** Estas intervenciones no computarán dentro de la bolsa anteriormente descrita. Salvo en el caso de actualizaciones de seguridad indicadas por el fabricante que operarán según la planificación del mismo, las actuaciones tendrán carácter al menos anual y siempre con la aprobación del Director del Proyecto por LA CONSEJERÍA.

8.5 RENOVACIONES DE LICENCIAS Y GARANTÍA

Tras la finalización del periodo de garantía exigido en este pliego se entenderá que los precios de TODAS LAS LICENCIAS relativas a los productos usados en el cortafuegos (piezas de software, firmas de virus, reglas de IDP / IPS, mecanismos de identificación…) no podrán superar los siguientes límites sobre el precio total de licitación durante los años de renovación 6, 7 y 8.

PRECIO TOTAL DE RENOVACIONES CON IVA DE LICENCIAS UTILIZADAS POR LA SOLUCIÓN CORTAFUEGOS, ENTENDIDO COMO MÁXIMO	**6,4 % DEL TOTAL DEL PRECIO DE LICITACIÓN POR AÑO.**

9 ACUERDO DE NIVELES DE SERVICIO

Con objeto de garantizar la calidad de los trabajos realizados, así como la pronta resolución de las incidencias que se produzcan en la plataforma que afecten a la disponibilidad de los sistemas gestionados se establecen los acuerdos de nivel de servicio detallados en este anexo.

9.1 INSTALACIÓN Y CONFIGURACIÓN

Para garantizar el cumplimiento de la planificación que se establezca en el proyecto de instalación y configuración se define el siguiente ANS:

ANS	Descripción	Valor
ANS1	Semanas de retraso en los trabajos planificados	< 1

	correspondientes a los hitos establecidos en el plan de facturación	

9.2 ADMINISTRACION DE LA PLATAFORMA

Se requiere la disponibilidad del soporte presencial y que éste se realice con el mismo técnico asignado por el adjudicatario tal y como se describe en el apartado anterior. Para garantizar estos requisitos se definen los siguientes acuerdos de servicio

ANS	Descripción	Valor
ANS2	Número de sustituciones no autorizadas del técnico asignado para prestar soporte presencial	< 1
ANS3	Días sin prestación de soporte presencial	< 2

Para las peticiones (ordenes de trabajo) los ANS se basarán en la complejidad de las tareas a realizar. Cada petición a realizar consta de un campo complejidad. En función del valor de dicho campo las tareas deberán de realizarse en un tiempo máximo prefijado que se detalla en la siguiente tabla:

Valor Complejidad	Descripción
Básica	Se estima un tiempo de ejecución < 3h
Media	Se estima un tiempo de ejecución entre 3h - 6h
Alta	Se estima un tiempo de ejecución entre 6h - 8h
n/a	Sin categorización

ANS	Descripción	Valor
ANS4	Porcentaje de Peticiones que se resuelven en los tiempos de especificados de acuerdo con la complejidad definida	> 95%

Los trabajos sin categorización se gestionarán como proyectos, requerirán estimación previa de la duración y planificación de los trabajos, y el cumplimiento de dicha planificación realizada. Se aplicará una penalización del 0,5% del importe de tasación del proyecto por cada día hábil de retraso en el proyecto. Si la ConsejerÍa lo estima oportuno se podrán realizar cambios en la planificación realizada para incluir aspectos no contemplados en la planificación inicial.

ANS	Descripción	Valor
ANS5	Dias de retraso en la ejecución de los proyectos planificados	< 2 dias

Los tiempos en los que deben resolverse las incidencias que se produzcan en los servicios prestados por las

infraestructuras dependerá del grado de afectación del servicio, la importancia de los sistemas afectados, el número de usuarios, etc. . Las incidencias se clasificarán con un valor que indicará el nivel de criticidad que definirá los tiempos en los que debe resolverse la incidencia, tal y como se expresa en la siguiente tabla:

ANS	Descripción	Valor
ANS6	Tiempo de resolución de incidencias de criticidad Alta	< 3horas
ANS7	Tiempo de resolución de incidencias de criticidad Media	>= 3horas y < 6horas
ANS8	Tiempo de resolución de incidencias de criticidad Baja	>= 6horas y <8horas

No se tendrá en cuenta a la hora de contabilizar los tiempos de resolución, los tiempos convenientemente justificados en el que se dependa de la actuación de un tercero para la resolución de la incidencia.

La siguiente tabla muestra ejemplos de clasificación de la criticidad de las incidencias según los componentes afectados:

INCIDENCIAS	HORARIO	CRITICIDAD
Caída total del servicio de SSCC y Hosting		ALTA
Caída de algún nodo de un cluster sin degradación del servicio		MEDIA
Caída total del Servicio sedes de tipo 3	Horario de Atención al Público (en la actualidad de Lunes a Viernes de 9:00 a 14:00)	ALTA
Caída total de Sedes tipo 1 y tipo 2	Horario Oficina	ALTA
Caída Sedes tipo 4	Horario oficina	MEDIA

9.3 GARANTÍA

Para garantizar el servicio de soporte vinculado con la garantía se establecen los siguientes ANS:

ANS	Descripción	Valor
ANS9	Tiempo de respuesta	< 4horas
ANS10	Tiempo de resolución Máximo	NBD (Next Business Day), En el siguiente día hábil al día en que se reporta la incidencia.

10 MEJORAS

10.1 CARACTERÍSTICAS DE SANDBOX

En las mejoras solicitamos que la solución de protección de la CONSEJERÏA sea integrada y también se deberá entregar completamente funcional atendiendo todos los requerimientos que se exponen en este pliego.

Se solicita un servicio ofrezca seguridad frente a amenazas desconocidas (*zero-day*) mediante el suministro, despliegue y configuración de una solución de análisis de amenazas avanzadas que debe cumplir con los siguientes requisitos:

- Deberá ser un equipo físico enracable en armario de 19 pulgadas.
- Deberá contar con un módulo de análisis dinámico (sandbox) basado en comportamiento y en el análisis real de las muestras en una VM.
- Deberá contar con un módulo de análisis estático para detectar aquel malware y exploits que trate de evadir el análisis dinámico, así como para identificar variantes de malware existente.
- Deberá apoyarse en técnicas de machine learning que permita aprender de las muestras analizadas para identificar nuevas variantes de malware que no es posible con análisis estático y dinámico.
- Deberá permitir la ejecución y análisis de muestras en hardware físico, para aquellas que se comporten de forma evasiva.
- Deberá generar nuevas firmas de protección en un plazo máximo de 5 minutos, que permitirán la reprogramación activa de la infraestructura perimetral.
- Deberá permitir la integración con algún servicio de inteligencia contextual de amenazas, para habilitar la posibilidad de hacer analítica y correlación de esa inteligencia de amenazas.
- Deberá poder compartir el veredicto generado a partir del análisis de las muestras con otras soluciones seguridad como de protección del puesto de trabajo, de protección del correo, con cortafuegos de red y de aplicaciones web, etc., de tal forma que éstas tengan cierta integración, desde el punto de vista de que los veredictos generados por muestras observadas en unas soluciones se utilicen para toma de decisiones en otras.
- Debe poder enviar los tipos de ficheros que defina el administrador (ejecutables .exe y .dll , imágenes, PDF, Office, javascript, ficheros comprimidos en .zip, .rar, gz…) a una plataforma de sandbox, de manera que sean analizados dichos ficheros y se de un veredicto sobre si son maliciosos o no.
- El sandbox ha de ser un servicio que realice múltiples técnicas de análisis (bases de datos extendidas de virus,

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 29 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

consulta a la comunidad del hash del fichero - por si ya ha sido analizado con anterioridad y ya es conocido- y ejecución en máquina virtual para analizar su comportamiento)

- Debe poderse analizar no sólo ficheros, sino también URLs en el sistema sandbox, para poder proteger de droppers y otras amenazas en la red con URLs maliciosas.

- El sandbox debe ser compatible con distintas imágenes de sistema operativo que puedan tener los usuarios corporativos. Para ello se requiere que sea compatible con imágenes de Windows XP, Windows 7, etc.

- El sandbox podrá ser cargado con imágenes personalizadas (Custom VMs) de sistemas operativos utilizados corporativamente como Windows 8, Windows 10 o distintas versiones de Windows Server.

- Se ha de poder analizar y detonar en las máquinas virtuales al menos 600 ficheros por hora sin pérdida de rendimiento.

- Con un mínimo de 5 máquinas virtuales diferentes..

- El sandbox debe poder ofrecer servicio de análisis forense, permitiendo la subida de ficheros o URL bajo demanda y generar una exhaustiva documentación respecto a la muestra que incluya: comportamientos de red, ficheros modificados, registros modificados, amenazas detectadas, etc.

- El sistema de análisis forense del sandbox debe ofrecer la capacidad de guardar un vídeo de la ejecución de la muestra, así como interactuar con la VM para replicar las acciones de los usuarios.

- El sistema sandbox se deberá poder integrar con la solución de seguridad del puesto de usuario de la CONSEJERIA (Symantec Endpoint)

La solución debe poder integrarse en una plataforma integral de seguridad que incorpore un sandbox para la protección frente a amenazas avanzadas, de modo que genere las firmas correspondientes para las muestras maliciosas recibidas, tanto para la actividad que la ejecución que dichas muestras genera (p.e. URLs, dominios DNS) como para la muestra en sí (p.e. PDFs, exe, etc). Dichas firmas deben poder ser desplegadas directamente sobre otros elementos de seguridad de red, del tipo Next Generation Firewall (NGFW) del mismo fabricante sin necesidad de ningún otro elemento.

Se requiere una solución de protección avanzada de nueva generación El sistema sandbox se deberá poder integrar con las distintas soluciones de puesto de usuario o proxies mediante el protocolo ICAP o integración nativa.

ANEXO 1. SISTEMA DE CORTAFUEGOS EN SSCC

Una descripción breve del actual sistema de cortafuegos es:

SUBSISTEMA DE CORTAFUEGOS:

El sistema de cortafuegos está compuesto por dos nodos en alta disponibilidad (ACTIVO-PASIVO) y un tercer

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 30 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

nodo de respaldo ante posibles contingencias.

El Software de cortafuegos es IPtables en la versión incluida en el sistema operativo instalado en los nodos.

En cuanto a la gestión del cortafuegos cuenta con un interfaz en software libre (preferiblemente FWBuilder) que permite la administración del subsistema.

El registro de actividad del sistema se exporta en tiempo real y de forma segura a una máquina de análisis de logs, desde la cual se mostrará mediante una interfaz web (accesible en modo texto) de la situación actual del sistema de seguridad.

Se cuenta además con:

.- Soporte Nat y Vlan tagging (802,11q)

.- Capacidad de creación de VPNs.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 31 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

ANEXO 2. SISTEMA DE CORTAFUEGOS EN HOSTING

Sus características técnicas, más relevantes, serían las siguientes: Se trata de un cortafuegos en activo-pasivo con conmutación manual basado en IPTables y en el que se han implementado, a fecha de hoy las siguientes Vlanes, con la vocación de seguir creciendo:

3.2.1 Interfaz tagged vlan de servicio [editar]

- Interfaz asociada: eth1
- Vlans:

```
- vlan400 configurada sin IP statica
- vlan405 configurada sin IP statica
- vlan410 configurada sin IP statica
- vlan415 configurada sin IP statica
- vlan420 configurada sin IP statica
- vlan425 configurada sin IP statica
- vlan430 configurada sin IP statica
- vlan435 configurada sin IP statica
- vlan440 configurada sin IP statica
- vlan445 configurada sin IP statica
- vlan450 configurada sin IP statica
- vlan455 configurada sin IP statica
- vlan460 configurada sin IP statica
- vlan465 configurada sin IP statica
- vlan470 configurada sin IP statica
- vlan475 configurada sin IP statica
- vlan480 configurada sin IP statica
- vlan489 configurada sin IP statica
- vlan490 configurada sin IP statica
- vlan491 configurada sin IP statica
- vlan492 configurada sin IP statica
- vlan493 configurada sin IP statica
- vlan494 configurada sin IP statica
- vlan495 configurada sin IP statica
- vlan496 configurada sin IP statica
- vlan497 configurada sin IP statica
- vlan498 configurada sin IP statica
- vlan499 configurada sin IP statica
```

ANEXO 3. SISTEMA DE CORTAFUEGOS EN DD.TT

Tabla de tipos de Sedes de las DD.TT y localizaciones periféricas. En cualquier caso todas las sedes son susceptibles de mejora inmediata en cuanto a ancho de banda que los dispositivos deberán ser capaces de gestionar. Concretamente es previsible que:

Correspondencia entre tipo sede / tipo dispositivo suministrable, número de sedes y su ubicación física:

Tipo de Sede Periférica.	Tipo de Dispositivo.	Ancho de banda conexión actual Red Corporativa.	Ancho de banda conexión previsible en Red Corporativa	Número.	Ubicación Provincial
Tipo 1	Tipo A	1Gb.	>1 Gb.	1	D.T. Sevilla
Tipo 2	Tipo A o Tipo B.	1Gb / 100 Mb.	>1 Gb.	7	Toda Andalucía.
Tipo 3	Tipo B ó Tipo C.	1 Gb / 100 Mb	1 Gb.	5	Toda Andalucía.
Tipo 4	Tipo C o tipo D.	Entre 100 Mb y 2 Mb.	1 Gb.	8	Toda Andalucía

Además se requiere, como se solicita en el epígrafe 5.1.5 SERVICIOS DE RED Link Aggregation Control Protocol IEEE 802.3ad, que permita la agregación de varias líneas / interfaces de 1 GB.

Las sedes de tipo 1, tipo 2 y tipo 3 deben constar, al menos, con dos nodos físicos que deben operar en modo “Alta Disponibilidad”, formando un cluster.

Los dispositivos tienen que tener la posibilidad de poder enracarse

Las siguientes especificaciones deberán considerarse como requisitos mínimos que deben cumplir los distintos dispositivos solicitados:

TIPO A

DISPOSITIVO	TIPO A
Número de sesiones concurrentes	3.2 Millones
Número de sesiones nuevas por segundo	300000
N.º de Politicas del Firewall	10000
Rendimiento de Firewall (1518 UDP Packets))	32
Rendimiento IPS	5 Gps
Rendimiento NGFW	3.5 Gbps
Rendimiento Protección contra Amenazas	3 Gbps
Interfaces	Al menos 8 GE RJ45

TIPO B

DISPOSITIVO	TIPO B
Número de sesiones concurrentes	2 millones
Número de sesiones nuevas por segundo	135000

JOSE DANIEL SOTO ALBA | 09/01/2020 | PÁGINA 33 / 38
VERIFICACIÓN | NJyGwRjA4DDQxOy2u52o4X8gCEFMAt | https://ws050.juntadeandalucia.es/verificarFirma

N.º de Politicas del Firewall	10000
Rendimiento de Firewall (1518 UDP Packets))	20 Gbps
Rendimiento IPS	2,2 Gbps
Rendimiento NGFW	1,8 Gbps
Rendimiento Protección contra Amenazas	1,2Gbps
Interfaces	Al menos 6 GE RJ45

TIPO C

DISPOSITIVO	TIPO C
Número de sesiones concurrentes	500000
Número de sesiones nuevas por segundo	30000
N.º de Politicas del Firewall	5000
Rendimiento de Firewall (1518 byte UDP Packets))	4 Gbps
Rendimiento IPS	400 Mbps
Rendimiento NGFW	350 Mbps
Rendimiento Protección contra Amenazas	250 Gbps
Interfaces	Al menos 5 GE RJ45

TIPO D

DISPOSITIVO	TIPO D
Número de sesiones concurrentes	500000
Número de sesiones nuevas por segundo	20000
N.º de Politicas del Firewall	5000
Rendimiento de Firewall (1518 / 512 / 64 byte UDP Packets))	2,5 Gbps
Rendimiento IPS	325 Mbps
Rendimiento NGFW	200 Mbps
Rendimiento Protección contra Amenazas	150 Gbps
Interfaces	Al menos 5 GE RJ45

Las tecnologías usadas en los cortafuegos de las DDTT de la Consejeria de Salud:

Tecnologías.	Observaciones.
Eneo.	
ClearOS.	

JOSE DANIEL SOTO ALBA | 09/01/2020 | PÁGINA 34 / 38
VERIFICACIÓN | NJyGwRjA4DDQxOy2u52o4X8gCEFMAt | https://ws050.juntadeandalucia.es/verificarFirma

ANEXO 4. PLAN DE PRUEBAS

El adjudicatario definirá y redactará un plan de pruebas a partir de los requerimientos que el Director del Proyecto por parte de LA CONSEJERÍA estime oportunos. Se facilitará un documento ejemplo o modelo de realización para tal tarea.

En general cada uno de los subsistemas o herramientas que componen las solución deberán de pasar un Plan de Pruebas que contenga, al menos, los siguientes puntos:

1 Pruebas a realizar antes de la puesta en producción: funcionalidad.
2 Pruebas a realizar antes de la puesta en producción: disponibilidad
3 Pruebas a realizar antes de la puesta en producción: rendimiento
4 Pruebas a realizar en producción: funcionalidad.
5 Pruebas a realizar en producción: disponibilidad.
6 Pruebas a realizar en producción: rendimiento.
7 Conjunto mínimo de pruebas a realizar el día de la migración.

El adjudicatario, según su criterio técnico, bajo la dirección del personal de LA CONSEJERÍA y siguiendo los modelos que se entreguen definirá las pruebas concretas a realizar en cada uno de los subsistemas o herramientas indicadas.

El Plan de Pruebas debe ser aplicable a cada uno de los dispositivos que se solicitan tanto en los SS.CC como en las DD.TT. Obviamente para los despliegues desasistidos en la DD.TT se proporcionará un plan de pruebas a seguir y a validar por el personal técnico de la Delegación Territorial.

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 35 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

ANEXO 5. SEDES Y LUGARES DE REALIZACIÓN DEL TRABAJO.

El reparto numérico de sedes según provincias es el siguiente:

PROVINCIA	SEDES
HUELVA	3
SEVILLA	4+ 1(SSCC)
CORDOBA	2
CADIZ	2
MALAGA	2
GRANADA	2
JAEN	3
ALMERÍA	3

Las direcciones de las distintas sedes que se atenderán con esta contratación son las siguientes:

Nombre Sede	Tipo De Vía	Dirección	Nº	Código Postal	Localidad
DELEGACION PROVINCIAL DE SALUD EN ALMERIA	C/	CARRETERA DE RONDA (DOCTOR FERRANZ)	7	04071	ALMERÍA
UNIDAD DE VALORACIÓN MÉDICA DE INCAPACIDADES DE AL	Ctra.	DE RONDA (EDIFICIO BOLA AZUL)	226	04004	ALMERÍA
OFICINA PROVINCIAL DE CONSUMO EN ALMERÍA	C/	HERMANOS MACHADO	4	04004	ALMERÍA
DELEGACION PROVINCIAL DE SALUD EN CADIZ	Avda.	MARIA AUXILIADORA	2	11009	CÁDIZ
UVMI CÁDIZ	Plaza	PLAZOLETA ARBOL	S/N	11008	CÁDIZ
DELEGACION PROVINCIAL DE SALUD EN CORDOBA ¿UVMI CÓ	Avda.	REPUBLICA ARGENTINA	34	14071	CÓRDOBA
OFICINA PROVINCIAL DE CONSUMO EN CÓRDOBA	C/	SANTO TOMÁS DE AQUINO	S/N	14004	CÓRDOBA
DELEGACIÓN PROVINCIAL DE SALUD EN GRANADA	Avda.	DEL SUR	11 Y 13	18014	GRANADA
OFICINA PROVINCIAL DE CONSUMO EN GRANADA	Avda.	DE MADRID	7	18012	GRANADA
DELEGACION PROVINCIAL DE SALUD EN HUELVA - UVMI	Avda.	MARTIN ALONSO PINZPN	6	21003	HUELVA
LABORATORIO DE SALUD PÚBLICA	Ctra.	SEVILLA (PABE. LOS ÁLAMOS, INFANTA ELENA)	S/N	21007	HUELVA
OFICINA PROVINCIAL DE CONSUMO EN HUELVA	Avda.	ESCULTORA MISS WITNEY	5	21003	HUELVA

JOSE DANIEL SOTO ALBA		09/01/2020	PÁGINA 36 / 38
VERIFICACIÓN	NJyGwRjA4DDQxOy2u52o4X8gCEFMAt	https://ws050.juntadeandalucia.es/verificarFirma	

DELEGACIÓN PROVINCIAL DE SALUD EN JAÉN	Paseo	DE LA ESTACION	15	23007	JAÉN
UVMI JAÉN	Avda.	DEL EJERCITO ESPAÑOL	10	23007	JAÉN
D.P. SALUD JAEN-LAB-CONSUMO	Paseo	DE LA ESTACIÓN	21	23071	JAÉN
DELEGACIÓN PROVINCIAL DE SALUD EN MÁLAGA	C/	CORDOBA	4	29001	MÁLAGA
LABORATORIO DE SALUD PÚBLICA	Avda.	MANUEL AGUSTÍN HEREDIA	34	29001	MÁLAGA
CONSEJERIA DE SALUD	Avda.	INNOVACION	S/N	41020	SEVILLA
DELEGACIÓN PROVINCIAL DE SEVILLA DE SALUD	Avda.	LUIS MONTOTO	87-89	41018	SEVILLA
U.V.M.I.: UNIDAD MÉDICA DE VALORACION E INCAPACIDADES	C/	MADRE DOLORES MARQUEZ	S/N	41003	SEVILLA
OFICINA PROVINCIAL DE CONSUMO EN SEVILLA	C/	LUIS MONTOTO	133	41007	SEVILLA
DIRECCIÓN GENERAL DE CONSUMO	Plaza	NUEVA	4	41001	SEVILLA

ANEXO 7. PLAN DE CONTINGENCIA

El Plan de Contingencia diseñado debe garantizar en todo momento y durante el tiempo que se estime por parte de la Dirección del Proyecto la posibilidad de vuelta atrás y retorno al sistema de cortafuegos anterior que debe de permanecer funcional y actualizado.

Obviamente ha de enfocarse la puesta en producción de la nueva herramienta de cortafuegos para tal fin atendiendo a ciertos criterios y guardas:

1. Mantener la actual infraestructura lógica y física en los nuevos cortafuegos.
2. Mantener el direccionamiento dispuesto actualmente.
3. No acometer durante la fase de retención cambios en la infraestructura de Vlanes o reflejarlos.
4. Establecer algún mecanismo histórico que permita cargar todos los cambios de reglas y política del nuevo cortafuegos en el sustituido.

Se entregará este plan de contingencia atendiendo a todas las prevenciones que se detallan en este Pliego y contendrá al menos:

1. Manual detallado del procedimiento de reversión a la infraestructura de cortafuegos original relatando minuciosamente todos los pasos a realizar.
2. Pruebas mínimas de funcionamiento del cortafuegos original restaurado.

Sevilla, a 9 de Enero de 2020

El Jefe de Informática

Fdo: José Daniel Soto Alba