Junta de Andalucía

CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA
Dirección General de Transformación Digital

Unión Europea

Fondo Europeo
de Desarrollo Regional

Pliego de Prescripciones Técnicas

"INFRAESTRUCTURA DE PROTECCIÓN DE ACTIVOS PARA LA CONSOLIDACIÓN TIC DE LA JUNTA DE ANDALUCÍA EN DOS CENTROS DE DATOS ACTIVO-ACTIVO". EXPTE. CONTR2020 366575, SGT068/20TIC.

Andalucía
se mueve con Europa

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 1 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

CONTENIDO

1 DEFINICIONES, ABREVIATURAS Y ACRÓNIMOS....4
2 INTRODUCCIÓN....5
3 OBJETO DEL PLIEGO....9
4 DESCRIPCIÓN DEL ENTORNO ACTUAL....9
5 PRESCRIPCIONES TÉCNICAS....9
5.1 Situación a alcanzar mediante la presente contratación....10
5.2 Requisitos generales....11
5.2.1 Conectorización y cableado....12
5.2.2 Monitorización....12
5.2.3 Arquitectura....13
5.3 Requisitos Funcionales y Técnicos....14
5.3.1 Sistema de cortafuegos (NGFW) [CICA y ZOCO]....15
5.3.2 Sistema de cortafuegos (NGFW) [Torretriana]....18
5.3.3 Sistema de balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas [CICA y ZOCO]....21
5.3.4 Sistema de acceso seguro a internet [CICA y ZOCO]....23
5.3.5 Sistema de almacenado y sellado de logs [CICA y ZOCO]....25
5.3.6 Sistema de gestión de eventos de seguridad. [CICA y ZOCO]....26
5.3.7 Herramienta de análisis de vulnerabilidades....28
5.4 Servicios y garantía técnica....29
5.4.1 Servicios de mantenimiento y soporte correctivo....29
5.4.2 Servicio de soporte avanzado....32
5.4.2.1 Consultoría sobre nuevas tecnologías de seguridad de la información....33
5.4.2.2 Servicio de monitorización de eventos de seguridad....33
5.4.2.3 Realización de pruebas de contingencia....33
5.4.3 Servicios de valor añadido....33
5.4.3.1 Servicio de auditoría y certificación de sistemas de información de la CHIE....34
5.4.3.2 Bolsa de horas de asistencia técnica....36
5.4.3.3 Bolsa de horas de auditoría....36
5.4.3.4 Bolsa de horas de formación....37
5.4.4 Servicios de capacitación técnica y transferencia de conocimiento....38
5.4.5 Gestión de proyecto....44
5.4.6 Plan de proyecto....46
5.4.6.1 Fases de ejecución del proyecto....47
5.4.7 Retirada y tratamiento medioambiental y seguro de los equipos....49
6 CONDICIONES GENERALES....50
6.1 Funciones y responsabilidades....50
6.2 Lugar de entrega de los suministros y transporte....50
6.3 Inventariado de los bienes suministrados....51
6.4 Medidas de información y publicidad (fondos FEDER)....51
6.5 Documentación entregable del proyecto....51
6.6 Formato de entregables....53
6.7 Confidencialidad....53

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 2 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

6.8 Conformidad con el Esquema Nacional de Seguridad.....54
6.9 Propiedad intelectual.....54
6.10 Esquema Nacional de Seguridad.....54

7 ANEXO. CLÁUSULAS GENÉRICAS DE PRODUCCIÓN APLICABLES.....56

7.1 Información para la Puesta en Explotación de la Infraestructura.....56
7.2 Aceptación de los trabajos.....56
7.3 Supervisión de los Sistemas.....56
7.4 Trazabilidad y auditoría.....57
7.5 Software base a utilizar. Software comercial. Licencias.....57

8 ANEXO. CLÁUSULAS GENÉRICAS DE SEGURIDAD APLICABLES.....59

8.1 Políticas y procedimientos de seguridad.....59
8.2 Cumplimiento medidas ENS.....59
8.3 Aspectos de seguridad a tener en cuenta para la Plataforma de Producción.....59
8.3.1 Accesos remotos.....59
8.3.2 Explotación y monitorización de sistemas.....60
8.3.3 Gestión de usuarios.....60
8.3.4 Protocolos de comunicaciones inseguros.....60

9 ANEXO: INSTALACIONES ELÉCTRICAS Y CABLEADO DE COBRE Y FIBRA.....61

9.1 INSTALACIÓN ELÉCTRICA RACKS.....61
9.2 CABLEADO DE COMUNICACIONES.....61
9.2.1 Enlaces.....61
9.2.2 Provisión de latiguillos de cobre y fibra.....63

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 3 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

1 DEFINICIONES, ABREVIATURAS Y ACRÓNIMOS

La Consejería: Consejería de Hacienda, Industria y Energía de la Junta de Andalucía.

CHIE: Consejería de Hacienda, Industria y Energía.

CPD: Centro de Proceso de Datos.

RCJA: Red Corporativa de la Junta de Andalucía

CICA: Sede ubicada en el Campus Universitario de Reina Mercedes, concretamente en la calle Tarfia.

ZOCO: Sede ubicada en Tomares, concretamente en la Avenida de la Arboleda

WAF: Web Application Firewall (Cortafuegos de Aplicaciones Web)

TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)

SO: Sistema Operativo

SSL: Secure Socket Layer (capa de puertos seguros)

SFP: Small form-factor pluggable (transceptor de factor de forma pequeño conectable)

SSD: Solid State Drive (Unidad de estado sólido)

HTTP: Hypertext Transfer Protocol (protocolo de transferencia de hipertexto)

TPS: Transactions per second (Transacciones por segundo)

DoS: Denial of Service (Denegación de servicio)

DDoS: Distributed Denial of Service (Denegación de servicio distribuido)

VRRP: Virtual Router Redundancy Protocol (Protocolo de redundancia de router virtual)

NAT: Network Address Translation (traducción de direcciones de red)

PAT: Port address translation (traducción de puertos de red)

TOR: The Onion Router (Encaminamiento/Enrutamiento de Cebolla, red de anonimato)

DHCP: Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host)

LDAP: Lightweight Directory Access Protocol (Protocolo Ligero/Simplificado de Acceso a Directorios)

NTLM: NT LAN Manager

OCSP: Online Certificate Status Protocol. Método de comprobación de estado de certificados

CRLDP: Certificate Revocation List Distribution Point. Lista de certificados revocados

FNMT: Fábrica Nacional de Moneda y Timbre

TACACS: Terminal Access Controller Access Control System (sistema de control de acceso mediante control del acceso desde terminales)

NGFW: Next Generation Firewall (cortafuegos de nueva generación)

IPS: Intrusion Prevention System (Sistema de prevención de intrusiones)

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 4 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

2 INTRODUCCIÓN

El presente documento es el Pliego de Prescripciones Técnicas (en adelante referido como Pliego) para determinar las condiciones para la contratación del suministro, instalación y configuración de elementos de seguridad de la información para varios CPDs de la Junta de Andalucía.

La operativa diaria de la Junta de Andalucía exige una disponibilidad en horario extendido para la mayor parte de los servicios, y, ademas, entre estos servicios se encuentran aquellos que como parte de Administración Electrónica están sometidos por imperativo legal a una disponibilidad cercana al 24x7.

La entrada en vigor de las leyes 39/2015 y 40/2015 añade si cabe mayores requisitos en cuanto a disponibilidad. Es por tanto obligado disponer de recursos que garanticen niveles de funcionamiento próximos al 24x7 los 365 días del año.

Los ciudadanos confían en que los servicios públicos disponibles por el medio electrónico se presten en unas condiciones de seguridad equivalentes o superiores a las que encuentran cuando se acercan personalmente a las oficinas de la Administración.

Por otra parte, las ciberamenazas, que constituyen riesgos que afectan singularmente a la Seguridad Nacional, se han convertido en un potente instrumento de agresión contra las entidades públicas y los ciudadanos en sus relaciones con las mismas, de manera que la ciberseguridad figura entre los doce ámbitos prioritarios de actuación de la Estrategia de Seguridad Nacional como instrumento actualizado para encarar el constante y profundo cambio mundial en el que nos hayamos inmersos y como garantía de la adecuada actuación de España en el ámbito internacional. En particular, dicho ámbito de actuación de ciberseguridad se refiere a la garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas y a que se finalizará la implantación del Esquema Nacional de Seguridad, de obligado cumplimiento tal y como indican las leyes 39/2015 y 40/2015. Profundizando en la cuestión, la Estrategia de Ciberseguridad Nacional «que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia» y en su línea de acción 2, titulada «Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas», se incluye la medida relativa a «Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados».

Por ello, se hace imprescindible gestionar la seguridad de las TIC, pues la confianza es un elemento fundamental a la hora de aprovechar las nuevas tecnologías, y sobre todo Internet, como soporte esencial de la actividad económica y social. Establecer un clima de confianza en el ámbito digital es una tarea compleja que precisa del compromiso de las administraciones, de las empresas y de la ciudadanía. Tal y como establece la Estrategia de Ciberseguridad de la Unión Europea, nuestra libertad y prosperidad dependen, cada vez más, de un ciberespacio abierto, protegido y seguro, correspondiendo a las administraciones públicas un papel destacado en la custodia del mismo.

Con el paso de los años se han incrementado el número, tipología y gravedad de los diferentes vectores de ataques contra los sistemas de información de las Administraciones Públicas y Gobiernos, de las empresas e instituciones de interés estratégico o aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos. La generalización del uso de los medios electrónicos incrementa la superficie de ataque y, en

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 5 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

consecuencia, los beneficios potenciales derivados, lo que constituye sin duda uno de los mayores estímulos para los atacantes.

El ciberespionaje ha constituido en los últimos años la mayor amenaza para los países, estando especialmente dirigida a los sistemas de información de las corporaciones industriales, empresas de Defensa, alta tecnología, automoción, transportes, instituciones de investigación y Administraciones Públicas. El ciberdelito, su profesionalización y el crecimiento de la organización interna de sus actores acaparan el siguiente nivel de atención. La sofisticación de las técnicas usadas, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios de delincuencia bajo demanda) y la pulcritud en la perpetración de tales acciones constituyen una preocupación en crecimiento. Del mismo modo, el denominado "Malware as a service" y el Cibercrimen como Servicio "CaaS Cybercrime-As-A-Service" ha incrementado su penetración y profesionalización, habiéndose percibido una cierta "competencia" entre los propios ciberdelincuentes, lo que obliga a sus autores a prestar a sus clientes un servicio cada vez más fiable.

Por tanto se necesitan nuevos elementos para mitigar estos ataques combinados, que inspeccionen el tráfico completo, den visibilidad sobre lo que ocurre en la red y sean capaces de gestionar grandes volúmenes de información correlacionando eventos y evitando un posible ataque antes de que se produzca. La Consejería dispone de algunos elementos de nueva generación capaces de detectar los ataques tradicionales, sin embargo se tienen carencias significativas en cuanto a rendimiento y funcionalidades dado el actual panorama de ciberseguridad mundial.

Como indica el Consejo Europeo en su política "Mejorar la ciberseguridad en toda la UE", se establecen planes para "prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones en Europa", igualmente indican que "los Estados miembros deberían disponer, ya en la actualidad o como resultado de esta estrategia, de estructuras para abordar la ciberresiliencia, la ciberdelincuencia y la ciberdefensa; deben asimismo alcanzar el nivel de capacidades requerido para resolver los ciberincidentes".

Es por ello, que se requiere de la adquisición de nuevos sistemas dentro del entorno de la seguridad TIC, que contribuyan a la mejora de la protección de los activos de información mediante el despliegue de mecanismos técnicos que aseguren el acceso, la integridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, informaciones y servicios utilizados en medios electrónicos.

El artículo 8 del Decreto 101/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Hacienda, Industria y Energía, establece que le corresponden a la Dirección General de Transformación Digital todas las funciones relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones en las Administraciones Públicas de Andalucía, así como las atribuciones previstas en el artículo 30 de la Ley 9/2007, de 22 de octubre.

En particular tiene atribuidas, entre otras, las siguientes funciones:

- La elaboración y aprobación de los planes estratégicos de consolidación de los sistemas de información y comunicaciones, así como la programación y asignación de recursos humanos, técnicos y económicos para la consecución de los objetivos corporativos y sectoriales planificados y que será necesario reordenar y centralizar partiendo de la situación actual distribuida.
- La creación, mantenimiento y explotación del Censo de Sistemas de Información e Infraestructuras de la Administración de la Junta de Andalucía.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 6 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- La propuesta, impulso, dirección, desarrollo y gestión de los sistemas e infraestructuras informáticas corporativos y sectoriales de la Administración de la Junta de Andalucía con especial referencia a la implantación de un modelo centralizado de infraestructuras, conforme a los planes estratégicos de consolidación elaborados.

Para la implantación del modelo centralizado de infraestructuras es imprescindible realizar un cambio de paradigma en la gestión de las infraestructuras y así poder ofrecer un modelo de servicios públicos centrados y diseñados para la ciudadanía. Actualmente el modelo de gestión de las infraestructuras se encuentra distribuido, tanto en el ámbito presupuestario como en la toma de decisión tecnológica y solamente se ha podido avanzar en la centralización de los contratos de mantenimiento de las infraestructura pasado el tiempo de garantía de las misma. Esta situación provoca ciertas ineficiencias en los diferentes ámbitos lo que dificulta desarrollar una estrategia unificada que permita conseguir una homogeneidad en las soluciones tecnológicas que mejoren las condiciones de sostenibilidad, disponibilidad, escalabilidad, seguridad y flexibilidad de los servicios soportados. A su vez este nuevo modelo mejorará la eficiencia y eficacia en la propia gestión de las infraestructuras, eliminando redundancias y duplicidades en las tareas, procesos y sistemas con el consecuente ahorro de costes.

La Dirección General de Transformación Digital ha iniciado los trabajos de consolidación de infraestructuras y servicios comunes con la intención de dar respuesta al objetivo de concentrar y racionalizar los servicios y las infraestructuras dentro del marco estratégico de transformación digital propuesto en la Junta de Andalucía. Actualmente estos trabajos se encuentran en la fase inicial de recogida de información procedente de los diferentes organismos con la intención de dar forma al modelo de consolidación más adecuado para la gestión de las infraestructuras. Asimismo, será necesario acometer, durante varios años, múltiples trabajos de muy diverso ámbito, entre los que se encuentran la adecuación del equipamiento, la evolución en la gestión de la infraestructura, la migración de servicios y la ejecución de traslados.

Por todo lo anterior, se hace necesario dotar a la Junta de Andalucía de una nueva Plataforma que permita la consolidación de los sistemas de información existentes en múltiples CPDs de las diferentes Consejerías y organismos, y que deberá incluir los múltiples componentes que formen parte de la plataforma con una serie de requisitos, que son objeto de descripción en el presente pliego.

En esta Plataforma de Consolidación se podrán migrar tanto sistemas de información ya existentes de las diferentes Consejerías desplegadas en sus CPDs, como desplegar sistemas de información nuevos, ofrecidos a través de un catálogo de servicios de provisión de recursos previamente establecido. De esta forma, se consigue:

- Homogeneización de las funciones de administración y operación, tanto de las aplicaciones existentes como de las nuevas aplicaciones
- Obtención de informes para las aplicaciones existentes.
- Obtención de un modelo de coste común, para facilitar la imputación de coste, de ambos tipos de aplicaciones.
- Ofrecer a las diferentes Consejerías las funciones de ‘día 2’ como valor añadido, también para las aplicaciones existentes.

La migración y consolidación de aplicaciones a la nueva Plataforma de consolidación empezará por las aplicaciones desplegadas en sede CICA y sede ZOCO.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 7 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Por los motivos expuestos y para garantizar la disponibilidad de los sistemas de información, la Consejería de Hacienda, Industria y Energía considera necesario renovar la infraestructura de seguridad de los CPDs de acuerdo a los objetos y contenidos que se detallan en el presente pliego.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 8 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

3 OBJETO DEL PLIEGO

El presente pliego técnico tiene como objetivo:

1. Suministro, instalación y configuración de una nueva infraestructura de protección de activos para los Centros de Datos de la Junta de Andalucía, así como los servicios profesionales necesarios para la migración de los actuales sistemas a los nuevos adquiridos, que incluye al menos estos sistemas:
   I. Sistema de cortafuegos de nueva generación (NGFW) en alta disponibilidad, al menos 1 clúster en CPD de CICA, otro clúster idéntico en CPD de ZOCO, y otro clúster adicional para la sede de CHIE sita en Edificio Torretriana también en HA.
   II. Sistema de balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas en alta disponibilidad, al menos 1 clúster en CPD de CICA y otro clúster idéntico en CPD de ZOCO.
   III. Sistema de navegación segura a internet en alta disponibilidad entre CPD de CICA y ZOCO.
   IV. Sistema de almacenado y sellado de logs en alta disponibilidad entre CPD de CICA y ZOCO.
   V. Sistema de gestión de eventos de seguridad en alta disponibilidad entre CPD de CICA y ZOCO.
   VI. Herramienta de análisis de vulnerabilidades.
2. Soporte y mantenimiento de todo el hardware suministrado en la presente licitación.
3. Soporte y mantenimiento de todo el software y licencias suministradas en la presente licitación.
4. Servicios de soporte avanzado.
5. Servicios de valor añadido.
6. Servicios de capacitación técnica y transferencia de conocimiento

Los objetos anteriores deberán cumplir con las características técnicas y funcionales mínimas que se indican en los próximos apartados.

4 DESCRIPCIÓN DEL ENTORNO ACTUAL

Debido al aumento del uso de técnicas OSINT (inteligencia de fuentes abiertas) para la recopilación de información por parte ciberdelincuentes y ciberespias, es necesario limitar la información de activos e infraestructura interna que se ofrece de manera pública, por tanto la información especifica acerca de la descripción de la infraestructura actual se entregará a las empresas licitadoras que así lo soliciten.

La solicitud de dicha documentación deberá realizarse mediante petición formal al organismo de contratación de la Junta de Andalucía mediante la cuenta de correo contratacion.chie@juntadeandalucia.es.

5 PRESCRIPCIONES TÉCNICAS

Las especificaciones aquí recogidas se entienden como las mínimas exigibles, haciéndose constar en su caso las que serán objeto de especial valoración.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 9 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

La contratación, a la que este Pliego sirve, incluye el suministro de sistemas y servicios diversos por su naturaleza, o por su ubicación, o por los plazos de entrega. En este sentido, cada uno de los diversos elementos se rige por las prescripciones que para el mismo se señalan en los correspondientes apartados siendo, no obstante, de aplicación a todos, lo que se exprese con carácter general salvo lo que no corresponda por la naturaleza del elemento o porque expresamente así quede dicho.

5.1 Situación a alcanzar mediante la presente contratación

Mediante esta contratación se pretende conseguir una infraestructura con nuevas funcionalidades[1] y de mayor capacidad que la actual en materias de ciberseguridad en la Consejería de Hacienda, Industria y Energía, una infraestructura que englobe al menos las funcionalidades de sistema de cortafuegos (NGFW), sistema de balanceo de carga, proxy de acceso a Internet y gestión centralizada de eventos e información de seguridad y que permita la consolidación de los sistemas de información existentes en múltiples CPDs de las diferentes Consejerías y organismos. Adicionalmente, se requiere de un software de análisis de vulnerabilidades que complemente las funcionalidades de seguridad de la presente contratación.

Así, los sistemas que se pretenden adquirir son los siguientes:

- **Sistema de cortafuegos de nueva generación** (NGFW) con alta disponibilidad y fiabilidad, junto a las funcionalidades típicas de un cortafuegos de nueva generación, prevención de intrusiones y antivirus perimetral de nueva generación con identificación de aplicaciones, usuarios y posibilidad de aplicación de políticas complejas sobre ellos, y en general, tratamiento de tráfico a nivel 7 de la capa OSI. Deberá ofertarse al menos un sistema para cada sede: CICA, ZOCO y Torretriana. Los de CICA y ZOCO, deberán ser idénticos.
- **Sistema de balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas.** Deberá ofertarse al menos un sistema para CICA y otro para ZOCO, que deberán ser idénticos.
- **Sistema de acceso seguro a Internet**. Este equipamiento proporcionará funcionalidades de seguridad que permitan el análisis y eliminación de código malicioso (antivirus) para entregar a los usuarios tráfico de Internet libre de este tipo de contenidos maliciosos. Deberá ofertarse al menos un sistema activo en cada CPD (CICA y ZOCO) y deberá proponerse una arquitectura de alta disponibilidad entre ambas ubicaciones.
- **Sistema de almacenado y sellado de logs en alta disponibilidad entre CPD de CICA y ZOCO**. Deberá ofertarse un sistema en alta disponibilidad entre CICA y ZOCO.
- **Sistema de gestión de eventos de seguridad en alta disponibilidad entre CPD de CICA y ZOCO.** Deberá ofertarse un sistema en alta disponibilidad entre CICA y ZOCO.
- **Herramienta de análisis de vulnerabilidades.**

Todos estos sistemas se deberán integrar entre ellos y así como con el resto de la infraestructura de la Junta de Andalucía. **Se deberán migrar las actuales configuraciones a los nuevos sistemas por parte del licitador**. Los sistemas deberán ser instalados y configurados con la última versión disponible y recomendada por el fabricante, tras conformidad de la Consejería.

1 Se entiende por nueva funcionalidad toda aquella característica del nuevo sistema que no estuviera ya presente en los actuales. EJ. Cortafuego sin posibilidad de actualizar, por tanto sin acceso a nuevas funcionalidades.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 10 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Con la presente contratación también se pretende adquirir los conocimientos necesarios para la administración de las posibles nuevas plataformas y funcionalidades ofertadas por el licitador, soporte avanzado y otros servicios de valor añadido.

A modo de **resumen**, la presente contratación engloba como **mínimo** los siguientes sistemas:

Sistemas	**N.º de equipos hardware**	**Sede**
Cortafuegos (NGFW)	2 en alta disponibilidad	CICA
Cortafuegos (NGFW)	2 en alta disponibilidad	ZOCO
Cortafuegos (NGFW)	2 en alta disponibilidad	Edificio Torretriana
Balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas	2 en alta disponibilidad	CICA
Balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas	2 en alta disponibilidad	ZOCO
Acceso seguro a Internet	Al menos 1 en cada CPD	CICA y ZOCO
Sistema de almacenado y sellado de logs.	Pueden ser virtuales, pero con condiciones de HA entre los 2 CPDs	CICA y/o ZOCO
Sistema de gestión de eventos de seguridad.	Pueden ser virtuales, pero con condiciones de HA entre los 2 CPDs	CICA y/o ZOCO
Herramienta de análisis de vulnerabilidades	No aplica al ser software	CICA y/o ZOCO

Igualmente se requieren, además de los servicios de puesta en marcha de los sistemas anteriores, los siguientes servicios:

Servicios	**Observaciones**
Servicios de mantenimiento y soporte correctivo	Sobre todos los sistemas incluidos del pliego
Servicio de soporte avanzado	Según se indica en apartados posteriores
Servicios de valor añadido	Según se indica en apartados posteriores
Servicios de capacitación técnica y transferencia de conocimiento	Según se indica en apartados posteriores

5.2 Requisitos generales

Deberá garantizarse la prestación adecuada de los servicios TIC actuales de la Junta de Andalucía sin que las actuaciones de instalación, puesta en marcha y traslado de servicios a la nueva infraestructura supongan paradas incontroladas de los mismos.

La Infraestructura ofertada deberá contar con las siguientes características generales:

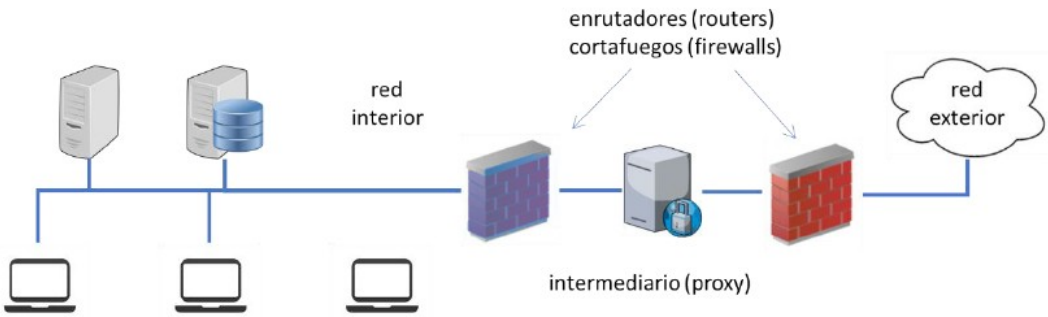
- Compatibilidad total con los servicios TIC actuales de la Junta de Andalucía.
- Alto nivel de disponibilidad, acorde con la criticidad, que iguale o incremente el nivel de disponibilidad actual, minimizando los puntos únicos de fallo.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 11 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Gestión y monitorización técnica avanzada, con máxima integración, que suponga el menor esfuerzo de administración posible.
- Nivel de flexibilidad alto, que permita responder a requerimientos cambiantes.
- Nivel adecuado de escalabilidad, que permita responder a requerimientos crecientes con un coste razonable.
- Máxima interoperabilidad, presente y futura.
- No se admitirán soluciones ni funcionalidades tipo "cloud", es decir, en las que algún dato tenga que salir fuera de la Junta de Andalucía para ser tratado o bien en las que algún componente de la solución no se encuentre en el CPD de la Junta de Andalucía, salvo en el caso del sistema SIEM.

Igualmente, con carácter general, se deberá respetar el esquema y funcionalidades de navegación y publicación de la Junta de Andalucía, que se expone a continuación y que se encuentra dentro del marco de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía:

- Siguiendo las recomendaciones recogidas en la Guía de Seguridad de las TIC CCN-STIC 811, la arquitectura de la infraestructura de seguridad del Nodo de InterconeXión Avanzado (NIXA en adelante), en lo referente a la navegación y publicación, es del tipo APP-6 "mejorada", ya que a dicha arquitectura se le ha añadido como mejora el requisito de que el fabricante de los firewall de primera línea de seguridad sea distinto a los de segunda línea.
- La publicación y navegación se realiza según el siguiente esquema, a través de los elementos proxy intercalados entre las dos líneas de cortafuegos y conectados a ambas por electrónica de red distintas:



- Con respecto al descifrado SSL o apertura de túneles SSL de publicación, se realizará siempre que no sea contraria al esquema de publicación de la RCJA.
- El adjudicatario deberá realizar en cualquier momento los cambios necesarios para adaptarse al esquema de publicación indicado anteriormente.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 12 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

5.2.1 Conectorización y cableado

Todas las conexiones entre los equipos ofertados, se realizarán con cables preconectorizados de fábrica con los conectores necesarios en cada caso y suministrados por el fabricante.

Se deberán seguir las indicaciones del anexo "Instalaciones eléctricas y cableado de cobre y fibra"

5.2.2 Monitorización

El objetivo de la monitorización es que el personal técnico de la Consejería disponga de información en tiempo real acerca de la situación de la infraestructura, incluyendo por tanto la identificación de eventos que puedan afectar a la prestación de los servicios.

Los sistemas de monitorización y control del rendimiento de utilizados están basados en los siguientes productos:

- Nagios Core 4.4.3
- Centreon v2.8.13.
- HP/Microfocus 10

La nueva infraestructura deberá monitorizarse al menos de la misma manera que la actual:

- Mediante envío de consultas y recepción de traps SNMP de los distintos dispositivos desplegados. El adjudicatario deberá proporcionar el soporte para el envío de consultas a los nuevos dispositivos desplegados.
- A través de consultas ICMP a los distintos dispositivos desplegados y consultas SNMP para control de CPU, memoria y estado del almacenamiento propio.
- El adjudicatario deberá realizar una propuesta de eventos a enviar a las herramientas de monitorización de la Consejería, incluyendo el significado de cada evento y de todas las variables del mismo.

Con carácter mínimo, deberán estar disponibles los siguientes datos:

- CPU
- Memoria
- Espacio en disco.
- Consumo de licencias cuando aplique
- Tasa de transferencia de las interfaces de red.
- Volúmenes de datos transferidos.

La plataforma deberá ser capaz de generar alertas en base a los datos de monitorización descritos. Estas alertas tendrán que quedar reflejada en la propia plataforma, pero de manera adicional podrán ser enviados fuera de la misma en base a los criterios que definan los administradores de la misma.

Como mínimo, la plataforma deberá tener la capacidad de enviar las alertas determinadas por los administradores por los siguientes métodos:

- Envío a un servidor externo de registros utilizando syslog, o syslog-ng, o rsyslog.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 13 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Envío de traps SNMP.
- Envío de correos mediante los servidores de correo corporativo de la Junta de Andalucía.

En el caso de que se desplieguen servidores/consolas dedicadas para gestión, administración o similares, y que sirvan como soporte para dar solución a los requisitos de monitorización y gestión incluidos en el presente pliego, se deberán monitorizar al menos el estado de CPU, memoria, almacenamiento y procesos críticos del sistema. Por ejemplo, si los sistemas de cortafuegos son administrados por una consola externa a los dispositivos cortafuegos, ésta consola debe ser igualmente monitorizable con el objeto de garantizar su disponibilidad y continuidad del servicio.

Los scripts/configuraciones necesarias para la integración con los sistemas de monitorización de la Consejería deberán ser proporcionadas por el adjudicatario.

En ningún caso se pondrá en producción un sistema que no esté integrado con la infraestructura de monitorización de la Consejería, por lo que con carácter previo a la puesta en explotación, debe estar definido y validado el procedimiento de monitorización, y probada y desplegada la monitorización.

5.2.3 Arquitectura

La arquitectura final de la solución a implantar y desplegar por el adjudicatario, se debe integrar con todos los sistemas existentes actualmente y con los que pudieran existir en las fases de ejecución del proyecto en los CPDs de la Junta de Andalucía (CICA, ZOCO y Torretriana).

En el caso de CICA y Zoco, debido a la necesidad de integración de todos estos sistemas en una arquitectura de CPDs activo-activo, y la existencia de varios escenarios posibles para dar dicho servicio, el licitador deberá entregar propuestas para, al menos, cada uno de estos escenarios y cualquier otro que considere oportuno, pudiendo ser adicional o híbrido entre ellos:

- Escenario 1.
  - CPDs activo-activo
  - Los 2 CPDs con salidas activas a la RCJA, permitiendo tráfico entrante y saliente en ambos sites.
  - Suponiendo que se permite conversar con protocolos de routing (tipo BGP) con el operador de RCJA.
  - Suponiendo la existencia de extensión LAN a nivel 2 entre los 2 CPDs (ya sea mediante técnicas a través de WAN o con fibra oscura o similar)
- Escenario 2.
  - CPDs activo-activo
  - Los 2 CPDs con salidas a la RCJA, pero no activas simultáneamente. Es decir, solo un CPD tiene salida activa a RCJA y por tanto, solo un CPD cursa tráfico entrante y saliente directo a RCJA.
  - Suponiendo que el mecanismo de conmutación lo aporta directamente el operador de RCJA.
  - Suponiendo la existencia de extensión LAN a nivel 2 entre los 2 CPDs (ya sea mediante técnicas a través de WAN o con fibra oscura o similar)
- Escenario 3.
  - CPDs activo-activo
  - Los 2 CPDs con salidas activas a la RCJA, permitiendo tráfico entrante y saliente en ambos sites.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 14 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Suponiendo que NO se permite conversar con protocolos de routing (tipo BGP) con el operador de RCJA.
- Suponiendo la existencia de extensión LAN a nivel 2 entre los 2 CPDs (ya sea mediante técnicas a través de WAN o con fibra oscura o similar)
- Suponiendo que se pueden publicar los servicios mediante mecanismos análogos a balanceo global por DNS.

En cada escenario indicar:

- Qué sistema/s de los ofertados se encargarían de cada función.
- Arquitecturas de red y esquemas generales de flujos de tráfico, características recomendadas (routing centralizado/distribuido, asimétrico/simétrico, solapamiento de vlans, direccionamientos compartidos, etc)
- Método y características de la interconexión entre los CPDs, tanto lógica como física.
- Principales ventajas e inconvenientes.
- Limitaciones y/o restricciones que cada sistema infiera.
- Indicando qué otro sistema distinto a los solicitados en la presente licitación, se necesitaría para llevar a cabo cada escenario (solo si aplica).

Adicionalmente, se indicará propuesta de orden de preferencia de los escenarios según el licitador, teniendo en cuenta la situación de la actual RCJA y los sistemas que se ofertan. No obstante, el escenario definitivo de implantación, lo decidirá la Dirección del Proyecto por parte de la Consejería.

5.3 Requisitos Funcionales y Técnicos

La nueva infraestructura de protección de activos debe incluir las características mínimas descritas a continuación, teniendo en cuenta que no solo deben tener la capacidad de soportarlas, sino que se deben entregar las correspondientes licencias para su uso inmediato y que dichas licencias deben ser perpetuas para la Consejería (sin pérdida de servicio a la finalización del soporte contratado), con la excepción de licencias de suscripción a servicios de actualización de firmas, categorías de urls o similares.

El licitador deberá incluir en los sobres 2 y 3 de la oferta el detalle del proceso de configuración de diversas funcionalidades de cada una de los sistemas ofertados. Dicho apartado deberá incluir, ademas de un texto explicativo, todas las capturas de pantalla de las interfaces de gestión de los sistemas necesarias para mostrar con detalle el proceso. Opcionalmente, se podrá entregar en soporte digital videos con audio con la descripción del proceso. El listado de los procesos de configuración a incluir, se especificará en el cuestionario del sobre 2 o 3 incluido en los anexos del PCAP según correspondan a criterios de valoración mediante formulas o criterios de valoración mediante juicios de valor.

La Consejería se reserva el derecho a solicitar al adjudicatario durante la ejecución del contrato la realización de una prueba de concepto con la configuración propuesta en la oferta, para comprobar que se cumple con las características requeridas en el pliego. El coste de dicha prueba será asumido por el adjudicatario y el resultado será vinculante en cuanto a realizar los cambios necesarios o adquisición del equipamiento hardware o software necesario para garantizar el cumplimiento de las características requeridas en el pliego

Se podrá excluir a los licitadores que no incluyan la descripción detallada de todos los procesos de configuración solicitados.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 15 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

5.3.1 Sistema de cortafuegos (NGFW) [CICA y ZOCO]

El adjudicatario suministrará e instalará todo el hardware, software y licencias necesarias para que el sistema de cortafuegos quede completamente operativo con todas las funcionalidades exigidas y ofertadas activadas.

En los siguientes requisitos se describen las funcionalidades y prestaciones que deben cumplir el sistema de cortafuegos y prevención de intrusiones. **Dichas funcionalidades y prestaciones deberán proporcionarse con un único equipo** (se solicitan 2 equipos idénticos por cluster en cada CPD (CICA y ZOCO) con la finalidad de proveer alta disponibilidad con los requisitos indicados).

- El sistema permitirá el funcionamiento en modo transparente y modo router.
- Cada cluster estará formado por al menos 2 equipos idénticos (mismo fabricante, modelo, versión, licencias, etc.) en alta disponibilidad (activo/pasivo o activo/activo), de forma que no haya pérdida ni degradación de servicio ante el fallo de alguno de los elementos del sistema.
- Ambos clúster deben ser idénticos (mismo fabricante, modelo, versión, licencias, etc.)
- El tiempo de conmutación en caso de fallo deberá ser inferior a 1 segundo.
- El fallo de uno de los equipos no podrá implicar pérdida de servicio, capacidades o funcionalidades.
- La sincronización de configuración de los elementos, así como la conmutación en caso de fallo, deberán ser automáticas.
- Cada equipo tendrá una ocupación máxima de 3U
- El equipo dispondrá, como mínimo, de:
  - 4 interfaces 100/1000/10G RJ45
  - 16 interfaces 1G/10G SFP/SFP+ (ópticas 10G LC)
  - 4 interfaces 40G/100G QSFP28 (ópticas 40G LC)
- Todos los puertos que disponga el equipo, deberán ser suministrados completamente operativos y licenciados, es decir, incluyendo todas las ópticas o adaptadores necesarios. Siempre que se soporte, las velocidades de estas ópticas o adaptadores deberán ser las indicadas anteriormente.
- Cada equipo dispondrá de al menos 2 fuentes de alimentación redundantes, intercambiables en caliente sin pérdida de servicio.
- El almacenamiento de cada equipo será con al menos dos discos duros de estado sólido (SSD) en RAID-1 y una capacidad mínima de 240GB cada disco.
- No estará limitado el número de usuarios simultáneos que puede soportar cada uno de los equipos, salvo por las restricciones impuestas por la superación de los siguientes límites de capacidad:
  - Conexiones concurrentes, con respuesta HTTP de 64 bytes: mínimo 8.000.000.
  - Nuevas conexiones por segundo, con respuesta HTTP de 64 bytes: mínimo 290.000.
  - El sistema debe permitir la aplicación de políticas de seguridad en función de aplicaciones de nivel 7 (facebook, dropbox, webex,etc.), y debe ser capaz de identificar al menos 1500 de este tipo de aplicaciones.
  - Escenario de rendimiento 1:
    - El equipo debe ofrecer un rendimiento de filtrado no inferior a 35Gbps con tráfico real, con el reconocimiento de aplicaciones activo.
  - Escenario de rendimiento 2:
    - El rendimiento de cada equipo, con todos los mecanismos de inspección de contenidos, filtrado, patrones y funcionalidades requeridas activas de forma simultanea

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 16 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

(identificación de aplicaciones, IPS, antivirus,...), a excepción de la inspección SSL, debe ser de 17Gbps o superior.

- El porcentaje de penalización en el rendimiento de la red (latencia) introducido por cada equipo deberá mantenerse constante con tasas de tráfico por debajo del rendimiento exigido.
- En caso de que alguna característica ofrezca diferentes datos de rendimiento en los datasheets oficiales para diferentes escenarios, se considerará siempre el peor valor del escenario.
- La Consejería se reserva la posibilidad de realizar durante todo el periodo mantenimiento del equipo mediciones del rendimiento en el entorno de producción, usando para ello el tráfico real generado por los diferentes sistemas de la Consejería. Las condiciones de esta medición serán las mismas de las que se definen para los escenarios de rendimiento 1 y 2. Si se determina mediante estas mediciones que el equipo no está proporcionando el rendimiento exigido, se proporcionará al adjudicatario la posibilidad de revisar la configuración/sw del equipo, aunque en ningún caso desactivando servicios obligatorios indicados en cada escenario de rendimiento.

  Si tras esta revisión se repite la prueba de rendimiento y se vuelve a repetir el incumplimiento, el adjudicatario procederá al incremento de la capacidad de proceso del equipo, bien mediante ampliación de licencias, módulos hardware de proceso de datos, o la sustitución del equipo en caso de ser necesaria por uno de una gama superior, de otro fabricante o cualquier forma que se asegure el rendimiento mínimo exigido en los escenarios de rendimiento 1 y 2.

- El equipo soportará dual stack IPv4 e IPv6 a nivel de transporte y a nivel de servicio, incluyendo todas las funcionalidades de filtrado de tráfico y amenazas e identificación de aplicaciones.
- El equipo deber ser capaz de inspeccionar el tráfico SSL correspondiente a la publicación, no navegación, identificando cualquiera de las aplicaciones sobre túneles SSL.
- El equipo proporcionará la funcionalidad de firewall desde nivel de red (nivel 3), hasta nivel de aplicación (nivel 7). De esta forma, se deben poder aplicar reglas en relación a direcciones IP (origen, destino), puertos TCP/UDP, y aplicaciones y sus parámetros (independientemente del puerto y/o URL que utilicen).
- Las políticas basadas en aplicaciones estarán integradas en las políticas principales, es decir, en una misma política se podrán incluir objetos de nivel 4 y de nivel 7.
- El equipo incorporará servidor de DHCP y posibilidad de configuración de DHCP relay aplicable de manera diferenciada a las diferentes interfaces de red tanto físicas como virtuales.
- El equipo permitirá la captura de paquetes con filtrado de IP, puertos, VLAN, redes virtuales, etc. Dichas capturas deben ser compatibles con las herramientas más extendidas de análisis de tráfico (tipo WireShark).
- El equipo aplicará control de antivirus y malware a todo el tráfico, o una selección del mismo, en base a una selección por aplicación, con independencia de puertos específicos.
- El equipo deberá, al menos, permitir la identificación de tráfico malicioso generado por malware existente en la red o intentos de explotación de vulnerabilidades conocidas, y aplicar automáticamente reglas de filtrado en el firewall para bloquear dicho contenido.
- El equipo debe ser capaz de identificar las aplicaciones de nivel 7 en el tráfico gestionado, independientemente del puerto y/o URL.
- El equipo debe ser capaz de aplicar políticas de seguridad en función del campo X-Forwarded-For de la cabecera HTTP

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 17 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- El equipo deberá permitir crear firmas personalizadas para la identificación de aplicaciones propietarias.
- El equipo deberá reconocer y controlar las sub-funciones dentro de las aplicaciones, tales como transferencias de ficheros, chat, etc.
- La identificación de aplicaciones y dispositivos deberá poder usarse en el resto de módulos del equipo (cortafuegos, gestión de ancho de banda, etc...) como medio para controlar el comportamiento de las aplicaciones y asegurar el cumplimiento de la política deseada.
- El equipo soportará la implementación de múltiples sistemas o dominios virtuales (al menos 12).
- En caso de configuración de instancias virtuales, todas las funcionalidades requeridas deberán poder usarse en todas las instancias sin necesidad de licencias adicionales.
- El equipo deberá ser capaz de identificar, como mínimo, 1500 aplicaciones distintas independientemente del puerto que utilicen. Se aceptarán como aplicaciones distintas las sub-aplicaciones, entendiendo éstas como funcionalidades diferenciadas de una aplicación que tienen entidad suficiente para separar su identificación de cara a su gestión y priorización. Deberán estar incluidas entre las aplicaciones identificadas y controladas:
  - P2P: Bittorrent (descarga / subida), eMule (descarga / subida), etc
  - Servicios de ficheros: Dropbox (descarga / subida), etc
  - Redes Sociales: Twitter (consulta / publicación), Facebook (chat /consulta / publicación / juegos / multimedia), etc
  - Mensajera instantánea: MSN, Google Talk / Hangouts (chat / llamadas/ video), Whatsapp (chat / transferencia archivos / llamadas), etc
  - Proxys anónimos: Tor, etc
  - Acceso remoto: TeamViewer, RDP, Logmein, VNC, etc
- El equipo debe proporcionar funcionalidades de gestión del ancho de banda en base a parámetros de red y aplicación
- Las políticas de gestión de ancho de banda deben permitir al menos fijar reservas de ancho de banda para tráfico seleccionado, límites de tráfico y priorizar un tráfico respecto a otro.
- Capacidad de identificación de los usuarios:
  - Se podrá configurar el acceso a la red desde los interfaces internos mediante un control de usuarios.
  - Se podrán detectar los intentos de conexión y mostrar un portal de autenticación.
  - Los métodos de gestión de usuarios al menos serán lista local de usuarios, directorio activo de Windows y servidor LDAP
- El sistema debe ser capaz de registrar todas las comunicaciones que gestiona. Al menos 1Tb para registro de logs.
- Todas las funcionalidades indicadas deberán de poder ser realizadas desde una interfaz de gestión gráfica.
- Los fabricantes propuestos han de disponer de una guía de seguridad del CCN-CERT para servir de ayuda a la configuración y explotación durante el periodo de servicio, para la instalación, operación y mantenimiento de los cortafuegos.

Se valorará que soporten las siguientes características:

- Posibilidad de configurar mediante la interfaz de gestión gráfica perfiles y/o métodos de autenticación para usuarios sea mediante doble factor con certificado digital de la FNMT/DNIe y usuario de directorio activo de Windows. Realizando comprobación de que el certificado

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 18 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

digital corresponda con el usuario de directorio activo. Posibilidad de usar dicha autenticación bajo un portal cautivo o similar, por ejemplo.

- Posibilidad de configurar mediante la interfaz de gestión gráfica políticas de seguridad basadas en geolocalización, y en concreto que permita en una única regla denegar el acceso con origen cualquier país que NO sea España.
- Posibilidad de definir mediante la interfaz de gestión gráfica listas de objetos dinámicos externas (URLs, IPs) y aplicación de políticas de seguridad basadas en dichos objetos.

5.3.2 Sistema de cortafuegos (NGFW) [Torretriana]

El adjudicatario suministrará e instalará todo el hardware, software y licencias necesarias para que el sistema de cortafuegos quede completamente operativo con todas las funcionalidades exigidas y ofertadas activadas.

En los siguientes requisitos se describen las funcionalidades y prestaciones que deben cumplir el sistema de cortafuegos y prevención de intrusiones. **Dichas funcionalidades y prestaciones deberán proporcionarse con un único equipo** (se solicitan 2 equipos idénticos por cluster con la finalidad de proveer alta disponibilidad con los requisitos indicados).

- El sistema permitirá el funcionamiento en modo transparente y modo router.
- Cada cluster estará formado por al menos 2 equipos idénticos (misma marca, modelo, versión, etc.) en alta disponibilidad (activo/pasivo o activo/activo), de forma que no haya pérdida ni degradación de servicio ante el fallo de alguno de los elementos del sistema.
- El tiempo de conmutación en caso de fallo deberá ser inferior a 1 segundo.
- El fallo de uno de los equipos no podrá implicar pérdida de servicio, capacidades o funcionalidades.
- La sincronización de configuración de los elementos, así como la conmutación en caso de fallo, deberán ser automáticas.
- Cada equipo tendrá una ocupación máxima de 2U
- El equipo dispondrá, como mínimo, de:
  - 12 interfaces 100/1000/10G RJ45
  - 8 interfaces 1G/10G SFP/SFP+ (ópticas 10G LC)
  - 4 interfaces 40G SFP+
- Todos los puertos que disponga el equipo, deberán ser suministrados completamente operativos y licenciados, es decir, incluyendo todas las ópticas o adaptadores necesarios. Siempre que se soporte, las velocidades de estas ópticas o adaptadores deberán ser las indicadas anteriormente.
- Cada equipo dispondrá de al menos 2 fuentes de alimentación redundantes, intercambiables en caliente sin pérdida de servicio.
- El almacenamiento de cada equipo será con al menos dos discos duros de estado sólido (SSD) en RAID-1 y una capacidad mínima de 240GB cada disco.
- No estará limitado el número de usuarios simultáneos que puede soportar cada uno de los equipos, salvo por las restricciones impuestas por la superación de los siguientes límites de capacidad:
  - Conexiones concurrentes, con respuesta HTTP de 64 bytes: mínimo 3.000.000.
  - Nuevas conexiones por segundo, con respuesta HTTP de 64 bytes: mínimo 100.000.
  - El sistema debe permitir la aplicación de políticas de seguridad en función de aplicaciones de nivel 7 (facebook, dropbox, webex,etc.), y debe ser capaz de identificar al menos 1500 de este tipo de aplicaciones.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 19 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Escenario de rendimiento 1:
  - El equipo debe ofrecer un rendimiento de filtrado no inferior a 7,5 Gbps con tráfico real, con el reconocimiento de aplicaciones activo.
- Escenario de rendimiento 2:
  - El rendimiento de cada equipo, con todos los mecanismos de inspección de contenidos, filtrado, patrones y funcionalidades requeridas activas de forma simultanea (identificación de aplicaciones, IPS, antivirus,...), a excepción de la inspección SSL, debe ser de 3,5Gbps o superior.
- El porcentaje de penalización en el rendimiento de la red (latencia) introducido por cada equipo deberá mantenerse constante con tasas de tráfico por debajo del rendimiento exigido.
- En caso de que alguna característica ofrezca diferentes datos de rendimiento en los datasheets oficiales para diferentes escenarios, se considerará siempre el peor valor del escenario.
- La Consejería se reserva la posibilidad de realizar durante todo el periodo mantenimiento del equipo mediciones del rendimiento en el entorno de producción, usando para ello el tráfico real generado por los diferentes sistemas de la Consejería. Las condiciones de esta medición serán las mismas de las que se definen para los escenarios de rendimiento 1 y 2. Si se determina mediante estas mediciones que el equipo no está proporcionando el rendimiento exigido, se proporcionará al adjudicatario la posibilidad de revisar la configuración/sw del equipo, aunque en ningún caso desactivando servicios obligatorios indicados en cada escenario de rendimiento.

  Si tras esta revisión se repite la prueba de rendimiento y se vuelve a repetir el incumplimiento, el adjudicatario procederá al incremento de la capacidad de proceso del equipo, bien mediante ampliación de licencias, módulos hardware de proceso de datos, o la sustitución del equipo en caso de ser necesaria por uno de una gama superior, de otro fabricante o cualquier forma que se asegure el rendimiento mínimo exigido en los escenarios de rendimiento 1 y 2.

- El equipo soportará dual stack IPv4 e IPv6 a nivel de transporte y a nivel de servicio, incluyendo todas las funcionalidades de filtrado de tráfico y amenazas e identificación de aplicaciones.
- El equipo deber ser capaz de inspeccionar el tráfico SSL correspondiente a la publicación, no navegación, identificando cualquiera de las aplicaciones sobre túneles SSL.
- El equipo proporcionará la funcionalidad de firewall desde nivel de red (nivel 3), hasta nivel de aplicación (nivel 7). De esta forma, se deben poder aplicar reglas en relación a direcciones IP (origen, destino), puertos TCP/UDP, y aplicaciones y sus parámetros (independientemente del puerto y/o URL que utilicen).
- Las políticas basadas en aplicaciones estarán integradas en las políticas principales, es decir, en una misma política se podrán incluir objetos de nivel 4 y de nivel 7.
- El equipo incorporará servidor de DHCP y posibilidad de configuración de DHCP relay aplicable de manera diferenciada a las diferentes interfaces de red tanto físicas como virtuales.
- El equipo permitirá la captura de paquetes con filtrado de IP, puertos, VLAN, redes virtuales, etc. Dichas capturas deben ser compatibles con las herramientas más extendidas de análisis de tráfico (tipo WireShark).
- El equipo aplicará control de antivirus y malware a todo el tráfico, o una selección del mismo, en base a una selección por aplicación, con independencia de puertos específicos.
- El equipo deberá, al menos, permitir la identificación de tráfico malicioso generado por malware existente en la red o intentos de explotación de vulnerabilidades conocidas, y aplicar

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 20 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

automáticamente reglas de filtrado en el firewall para bloquear dicho contenido.

- El equipo debe ser capaz de identificar las aplicaciones de nivel 7 en el tráfico gestionado, independientemente del puerto y/o URL.
- El equipo debe ser capaz de aplicar políticas de seguridad en función del campo X-Forwarded-For de la cabecera HTTP
- El equipo deberá permitir crear firmas personalizadas para la identificación de aplicaciones propietarias.
- El equipo deberá reconocer y controlar las sub-funciones dentro de las aplicaciones, tales como transferencias de ficheros, chat, etc....
- La identificación de aplicaciones y dispositivos deberá poder usarse en el resto de módulos del equipo (cortafuegos, gestión de ancho de banda, etc...) como medio para controlar el comportamiento de las aplicaciones y asegurar el cumplimiento de la política deseada.
- El equipo deberá ser capaz de identificar, como mínimo, 1500 aplicaciones distintas independientemente del puerto que utilicen. Se aceptarán como aplicaciones distintas las sub-aplicaciones, entendiendo éstas como funcionalidades diferenciadas de una aplicación que tienen entidad suficiente para separar su identificación de cara a su gestión y priorización. Deberán estar incluidas entre las aplicaciones identificadas y controladas:
  - P2P: Bittorrent (descarga / subida), eMule (descarga / subida), etc
  - Servicios de ficheros: Dropbox (descarga / subida), etc
  - Redes Sociales: Twitter (consulta / publicación), Facebook (chat /consulta / publicación / juegos / multimedia), etc
  - Mensajera instantánea: MSN, Google Talk / Hangouts (chat / llamadas/ video), Whatsapp (chat / transferencia archivos / llamadas), etc
  - Proxys anónimos: Tor, etc
  - Acceso remoto: TeamViewer, RDP, Logmein, VNC, etc
- El equipo debe proporcionar funcionalidades de gestión del ancho de banda en base a parámetros de red y aplicación
- Las políticas de gestión de ancho de banda deben permitir al menos fijar reservas de ancho de banda para tráfico seleccionado, límites de tráfico y priorizar un tráfico respecto a otro.
- Capacidad de identificación de los usuarios:
  - Se podrá configurar el acceso a la red desde los interfaces internos mediante un control de usuarios.
  - Se podrán detectar los intentos de conexión y mostrar un portal de autenticación.
  - Los métodos de gestión de usuarios al menos serán lista local de usuarios, directorio activo de Windows y servidor LDAP
- El equipo debe ser capaz de registrar todas las comunicaciones que gestiona.
- Todas las funcionalidades indicadas deberán de poder ser realizadas desde una interfaz de gestión gráfica.
- Los fabricantes propuestos han de disponer de una guía de seguridad del CCN-CERT para servir de ayuda a la configuración y explotación durante el periodo de servicio, para la instalación, operación y mantenimiento de los cortafuegos.

Se valorará que soporten las siguientes características:

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 21 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Posibilidad de configurar mediante la interfaz de gestión gráfica perfiles y/o métodos de autenticación para usuarios sea mediante doble factor con certificado digital de la FNMT/DNIe y usuario de directorio activo de Windows. Realizando comprobación de que el certificado digital corresponda con el usuario de directorio activo. Posibilidad de usar dicha autenticación bajo un portal cautivo o similar, por ejemplo.
- Posibilidad de configurar mediante la interfaz de gestión gráfica políticas de seguridad basadas en geolocalización, y en concreto que permita en una única regla denegar el acceso con origen cualquier país que NO sea España.
- Posibilidad de definir mediante la interfaz de gestión gráfica listas de objetos dinámicos externas (URLs, IPs) y aplicación de políticas de seguridad basadas en dichos objetos.

5.3.3 Sistema de balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas [CICA y ZOCO]

El adjudicatario suministrará e instalará todo el hardware, software y licencias necesarias para que el sistema de balanceo de carga quede completamente operativo con todas las funcionalidades exigidas y ofertadas activadas.

En los siguientes requisitos se describen las funcionalidades y prestaciones que deben cumplir el sistema de balanceo de carga. **Dichas funcionalidades y prestaciones deberán proporcionarse con un único equipo** (se solicitan 2 equipos idénticos por cluster en cada CPD (CICA y ZOCO) con la finalidad de proveer alta disponibilidad con los requisitos indicados). No se admitirán soluciones que necesiten equipos adicionales para cubrir alguna funcionalidad concreta.

Se requiere una solución de balanceo de carga que permita integrar las siguientes funcionalidades:

- Gestión y balanceo de tráfico de aplicaciones
- Aceleración de tráfico
- Autenticación avanzada de usuarios
- El sistema estará formado por al menos 2 equipos físicos idénticos por cluster (misma marca, modelo, versión, etc.) en alta disponibilidad (al menos activo/pasivo), de forma que no haya pérdida ni degradación de servicio ante el fallo de alguno de los elementos del sistema.
- Ambos clúster deben ser idénticos (misma fabricante, modelo, versión, licencias, etc.)
- Cada uno de estos dos equipos cumplirá con las siguientes especificaciones:
  - El tiempo de conmutación en caso de fallo deberá ser inferior a 1 segundo.
  - La sincronización de configuración de los elementos, así como la conmutación en caso de fallo, deberán ser automáticas.
  - El equipo tendrá una ocupación máxima de 1U.
  - Throughput de 40 Gbps por nodo a nivel 7
  - Aceleración SSL 40 mil TPS (claves RSA de 2k)
  - Conexiones concurrentes a nivel 4: 80 millones.
  - Mínimo de 4 puertos QSFP+ (40G) por nodo (adaptadores de fibra LC)
  - Mínimo de 8 puertos SFP+ (10G) por nodo (adaptadores de fibra LC)
  - Todos los puertos que disponga el equipo, deberán ser suministrados completamente operativos y licenciados, es decir, incluyendo todas las ópticas o adaptadores necesarios. Siempre que se soporte, las velocidades de estas ópticas o adaptadores deberán ser las indicadas anteriormente.
  - El equipo dispondrá de al menos 2 fuentes de alimentación redundantes, intercambiables en caliente sin pérdida de servicio.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 22 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Los discos duros deberán ser de estado sólido (SSD).
- El equipo soportará la implementación de múltiples sistemas o dominios virtuales (al menos 12).
- En caso de configuración de sistemas o dominios virtuales, todas las funcionalidades requeridas deberán poder usarse en todas los sistemas o dominios sin necesidad de licencias adicionales.
- Debe disponer de capacidades de integración con entornos de virtualización de red mediante los protocolos VXLAN y NVGRE.
- Se podrá balancear en distintos segmentos de red
- Permitirá arquitectura de balanceo de carga a nivel 2 y/o nivel 3
- Soporte al menos de métodos de balanceo Round Robin (RR), Least Connections (LC), Fastest Response, Weighted RR, Weighted LC y métodos estadísticos basándose en el número de conexiones y la rapidez de respuesta.
- Se podrá finalizar tuneles SSL iniciados por los clientes, así como crear tuneles SSL entre el equipo y las granjas de servidores, en ambos casos, en distintos segmentos de red
- Soporte de persistencia configurable (IP origen, puerto origen, cookies, MSRDP, SIP, cabecera http, identificador SSL. También debe generar persistencia por parámetros del payload. Debe de tener capacidad de inspección del payload en TCP y UDP.)
- Permitirá la creación de scripts personalizados que se puedan aplicar a los servicios virtuales de forma que se pueda generar un árbol de comportamiento y decisión complejo frente a las conexiones entrantes en un servicio virtual concreto, con capacidad de gestionar dicha decisión al aceptar la conexión cliente, al inicio de la conexión HTTP, al recibir la respuesta del servidor real o a la ejecución primaria de dicho script. Deberá ser una solución abierta y programable que permita, entre otros:
  - Inspección completa del "payload"
  - Lenguaje relacional y basado en eventos
  - Permitirá el control para habilitar, orientar y cambiar de forma condicional el comportamiento de las aplicaciones.
  - Transformación selectiva del contenido sin necesidad de utilizar terceros equipos ni adquisición de licencias adicionales
  - Soporte de reescritura de Url y Uri
- Aceleración de servicios mediante técnicas de caching, multiplexación TCP y gestión de ancho de banda.
- La solución debe disponer de funcionalidades de autenticación de usuarios, que permitan la integración de la solución, con los diferentes sistemas de autenticación requeridos por las aplicaciones, permitiendo consolidar y centralizar sobre esta solución, la autenticación, autorización y auditoria de los usuarios cuando acceden a las aplicaciones publicadas
- La solución debe permitir la protección de las aplicaciones y servicios web ante ataques a nivel de aplicación y ataques de denegación de servicio y de manera proactiva (Web Application Firewall). Al menos con estas características:
  - Modo transparente (sin corte) de aprendizaje.
  - Que cubra TOP 10 de OWASP.
- Balanceo global de DNS. La solución debe permitir alta disponibilidad de aplicaciones distribuidas en 2 o más CPDs, con al menos estas características:
  - Balanceo estático y dinámicos.
  - Persistencia a nivel global.
  - Balanceo de carga según ubicación geográfica.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 23 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

        - Balanceo de servidores DNS.
        - Funcionamiento como DNS autoritativo de alto rendimiento.
    - Capacidad de realizar proxificación segura de tráfico ICA (Citrix) sin limitación de usuarios concurrentes con integración de la autenticación de dichos usuarios contra un AD de Microsoft, de forma que reemplace las funcionalidades de Citrix Web Interface o los servidores Storefront.
    - Generación de página de estado y consultas de parámetros de configuración: la solución propuesta debe incluir un sistema, método o scripts personalizados que obtenga toda la configuración de servicios balanceados, pools de servidores, puertos, estado de los miembros, perfiles aplicados, etc. y la muestre a través de una página web sencilla securizada y accesible mediante autenticación con, al menos, AD de Microsoft.
    - Todas las funcionalidades requeridas deben ser realizadas en un mismo equipo a excepción de la integración/simulación de Citrix y la generación de página de estado y consultas de parámetros de configuración.

Se valorará que soporten las siguientes características:

- Posibilidad de configurar mediante la interfaz de gestión gráfica la proxificación segura de tráfico ICA (Citrix) sin limitación de usuarios concurrentes con integración de la autenticación de dichos usuarios contra un AD de Microsoft, de forma que reemplace las funcionalidades de Citrix Web Interface o los servidores Storefront, en el mismo equipo que el resto de funcionalidades del apartado "5.3.3 Sistema de balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas [CICA y ZOCO]"
- Capacidad de virtualizar la plataforma hardware con al menos 12 sistemas o dominios virtuales con versiones de sistema operativo independientes y reservas/asignación fijas de recursos físicos.
- Funcionalidades avanzadas de WAF, todas mediante interfaz de gestión gráfica: firmas personalizadas, uso del campo X-FORWARDED-FOR como IP origen, aplicación de políticas por servicio virtual y auditoría de cambios.

5.3.4 Sistema de acceso seguro a internet [CICA y ZOCO]

La solución de navegación segura para los usuarios de la CHIE, trata dar respuesta a todo tipo de amenazas e incidencias tanto de cara a la seguridad como a la categorización de las distintas ubicaciones que son visitadas por los usuarios. Además, controla el acceso de los usuarios y debe generar informes semanales de la navegación especificando las categorías de los sitios visitados por cada usuario hacia internet.

La solución de navegación segura para los usuarios de la CHIE debe cumplir con los siguientes requisitos mínimos:

- Capacidad para soportar al menos 1000 usuarios concurrentes, teniendo en cuenta que se da servicio a más de 1700 usuarios y además a otros dispositivos sin autenticación.
- Capacidad de gestionar un tráfico de al menos 600 Mbps
- Doble fuente de alimentación al reemplazable en caliente
- Todos los puertos que disponga el equipo, deberán ser suministrados completamente operativos y licenciados, es decir, incluyendo todas las ópticas o adaptadores necesarios.
- Posibilidad de configuración como proxy transparente y como proxy explícito

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 24 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Capacidad de servir cualquier tipo de tráfico de streaming de video y audio.
- Autenticación de usuarios mediante directorio activo de windows, ldap, radius, etc
- La solución propuesta debe permitir el control de la descarga de ficheros, en función del usuario/grupo, la categoría de la URL, etc.
- La solución propuesta debe incorporar un servicio de categorización y multicategorización web (una misma web que pertenezca a 2 categorías), que realice la categorización en base a URL completa y no solo en base al sitio web.
- La solución debe soportar el uso de listas de URLs y/o IPs dinámicas de terceros, como por ejemplo fuentes de Office 365.
- La solución propuesta debe permitir definir políticas de control y seguridad sobre aplicaciones web 2.0, tales como Gmail, LinkedIn, YoutTube, FaceBook, Twitter, DropBox, iCloud, Cloud, Amazon Cloud Drive, Google Drive, WeTransfer, SkyDrive, Google Docs, WebEx, LogMeIn, NetFlix, etc... así como sobre operaciones individuales de esas aplicaciones.
- Posibilidad de realizar políticas en función de las horas y días de la semana.
- Posibilidad de mostrar páginas de bloqueo personalizadas según el tipo de excepción generada en la navegación.
- La solución propuesta debe poder configurarse y estar dimensionada para inspeccionar en busca de malware el 100% de los ficheros descargados como resultado de todas las peticiones http, independiente de la reputación del sitio web desde el que se descargaron.
- La solución propuesta, debe permitir escanear los ficheros recibidos con hasta 2 motores de anti-virus con heurísticos, de dos fabricantes diferentes.
- La solución propuesta debe ser capaz de inspeccionar el contenido de ficheros comprimidos, incluso cuando se empleen varios niveles de compresión.
- La solución propuesta debe permitir definir las acciones a realizar (tales como permitir o denegar) cuando un fichero no pueda ser escaneado por diferentes motivos, como por ejemplo cuando estén protegidos por contraseña.
- La plataforma de control y seguridad de la navegación propuesta, debe registrar en log cada una de las transacciones procesadas.
- La plataforma de control y seguridad de la navegación propuesta debe poder configurarse para que suba automáticamente los ficheros de log a uno o varios sistemas externos, para el post-procesamiento de los logs y su almacenamiento.
- Control de ancho de banda: La solución deberá permitir el control de Ancho de Banda al menos de aplicaciones de streaming.
- Generación de Informes: la solución propuesta debe incluir un sistema centralizado de generación de informes que, a partir de los logs detallados generados por la plataforma de control y gestión de la navegación permita genere bajo demanda y también de forma programada informes de navegación por usuario, grupo, URL, servidor de destino, categoría, aplicación web 2.0, tráfico permitido, tráfico bloqueado, nombre de fichero, etc. El sistema centralizado de generación de informes debe cumplir además los requisitos siguientes:

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 25 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Integración con servidor de email corporativo para la generación automática de informes.
- Generación de reportes semanales por cada usuario y envío del mismo a la dirección de correo electrónico que esta asociada a dicho usuario en directorio activo

- Todas las funcionalidades requeridas deben ser realizadas en un mismo equipo a excepción de la visualización de logs y la generación de reportes, que pueden realizarse en un sistema independiente.

5.3.5 Sistema de almacenado y sellado de logs [CICA y ZOCO]

El objetivo del sistema es la centralización de logs, no solo de la infraestructura ofertada, si no también para otros de sistemas de la infraestructura de consolidación de Junta de Andalucía.

Este componente es el encargado de asegurar la integridad y custodia de los logs durante el proceso de recogida y durante el tiempo que deban ser conservados para cumplir con la política de retención de logs (y por ende, con las regulaciones vigentes en dicha materia). Por otro lado, tiene como misión asegurar que la información almacenada esté disponible para su consulta y uso como evidencia digital con plena validez legal.

La guardia de los logs se realizará en el propio formato en que es generado por la fuente (formato nativo o raw-logs).

Se añadirá una marca de tiempo a los logs almacenados, para poder secuenciarlos temporalmente, además de esta marca de tiempo, este módulo debe implementar funciones para asegurar la integridad de los logs almacenados así cómo soportar el firmado digital para garantizar esta integridad.

Se aceptarán tanto soluciones de código abierto como soluciones comerciales.

Las características de este sistema deben cumplir al menos:

- Cumplimiento del punto op.exp.10 (protección de los registros) del Esquema Nacional de Seguridad.
- Los certificados y los mecanismos de cifrado utilizados por la solución deberán estar reconocidos por el Centro Criptológico Nacional.
- Debe soportar la recolección de logs de forma segura de al menos las siguientes fuentes de datos de la Junta de Andalucía:
  - Integración con el resto de plataformas incluidas en la oferta (Cortafuegos, balanceadores y proxy de acceso a internet)
  - Integración con servidores con sistema operativo Windows
  - Integración con servidores con sistema operativo Linux (Redhat, Centos, Fedora,etc)
  - Integración con servidores con sistema operativo Solaris
  - Integración con equipos de electrónica de red (al menos Dell y HP)
  - Integración con otros equipos o sistemas que usen syslog para el envío de logs
  - Integración con servidores y buzones de correo
  - Integración con Office 365

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 26 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Se deberán suministrar todas las licencias necesarias para soportar todas las fuentes indicadas anteriormente.
- Soporte de al menos 150GB de logs diarios
- Soporte para al menos 500 fuentes de logs. No se considerarán fuentes distintas a los distintos logs enviados por un mismo sistema (p. ej. auth.log, syslog.log en un mismo servidor solo computarán como una fuente de las 500 requeridas).
- Almacenamiento y retención de logs de al menos 1 año
- Posibilidad de consulta en tiempo real de todos los registros de los últimos 30 días.
- Posibilidad de configurar distintos tiempos de retención en función del tipo de fuente.
- Posibilidad de archivar los registros más antiguos en un almacenamiento externo, con posibilidad de poder recuperarlos desde dicho almacenamiento y visualizarlos en la consola del sistema para posibles análisis forenses.
- Posibilidad de reenviar en tiempo real logs a otros sistemas de forma selectiva, como por ejemplo a un sistema de gestión de eventos de seguridad, limitando el rate de flujo de logs reenviados.
- Posibilidad de establecer roles y políticas de acceso a los logs de las distintas fuentes dependiendo de cada usuario.
- Asegurar el cumplimiento normativo (ENS) acerca de la no modificación de los registros.
- El sistema a suministrar será en formato virtual compatible con la infraestructura virtual de la Consejería (Vmware) y no podrá tener limitaciones en cuanto al espacio en disco asignado a la máquina virtual.
- Soporte de alta disponibilidad entre los CPDs de CICA y ZOCO
- El centro de respuesta a incidentes de seguridad AndalucíaCERT se podrá integrar en este sistema para tareas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía. En concreto:
    - Se atenderán las solicitudes de acceso al sistema desde el CSIRT AndalucíaCERT, proporcionando usuarios de consulta.
    - Se atenderán las peticiones que lleguen desde AndalucíaCERT para duplicación y reenvío de tráfico, eventos y alertas a los sistemas de monitorización del CSIRT autonómico.

En cualquier caso este sistema, indistintamente de si es una solución de código abierto o un producto comercial, será instalado y configurado por parte del licitador, entregando una solución integrada en la infraestructura con las fuentes de eventos que decida la propia Consejería y de acuerdo a las características indicadas anteriormente.

Este sistema podría darse conjuntamente con el de gestión de eventos de seguridad.

5.3.6 Sistema de gestión de eventos de seguridad. [CICA y ZOCO]

La sofisticación de los ataques hace cada vez más necesario aportar visibilidad sobre el resultado de los mismos y los elementos comprometidos por lo que la capacidad de detectar y gestionar incidentes se convierte en un proceso crítico, tanto en remediación como inteligencia de amenazas.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 27 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

El objetivo del sistema es gestionar la seguridad corporativa de manera más eficiente, contando con visibilidad y protección unificada en todas las superficies de ataque, tanto en aquellas más recientes como la nube (pública y privada) como en las tradicionales, pasarela, dispositivos móviles, etc.

Se pretenden mejorar las capacidades para identificar los principales vectores de ataque que pueden afectar a la Junta de Andalucía, analizando y cruzando a información de los sistemas que se integren, incorporando registros de seguridad de diversas fuentes.

Se aceptarán tanto soluciones de código abierto como soluciones comerciales.

Las características de este sistema deben cumplir al menos:

- Debe soportar la recolección de eventos de al menos las siguientes fuentes de datos de la Consejería:
  - Todos los sistemas indicados en el punto anterior de almacenado y sellado de logs.
  - El propio sistema de almacenado y sellado de logs.
  - Flujos de tráficos de red
- Se deberán suministrar todas las licencias necesarias para soportar todas las fuentes indicadas anteriormente.
- Soporte para los siguientes protocolos de intercambio de eventos entre las fuentes y el sistema de recolección:
  - SNMP
  - SYSLOG
  - Flujos de red Netflow o IPFIX
  - Push/pull de ficheros en texto y descarga de información desde URL
  - Fuentes externas en formatos XML, TXT y CSV
- Soporte de al menos 3000 EPS por segundo, independientemente del número de fuentes.
- Monitorización y correlación de eventos en tiempo real.
- Deberá contar con una librería de casos de uso (reglas de correlación) específicos para fuentes de eventos particulares.
- Almacenamiento y retención de eventos de al menos 90 días.
- Deberá contar suscripción a servicios de inteligencia de ciberamenazas que proporcionen indicadores (IPs, URLs etc.) para la detección y enriquecimiento de los eventos.
- Creación y gestión de informes predefinidos y personalizables sobre: ataques, virus, eventos, uso de servicios y recursos (correo, web, ancho de banda, entre otros).
- Interfaz de gestión web basada en usuarios y contraseñas
- Control de acceso y autenticación basada en directorio activo de windows
- Asignación de privilegios a usuarios basada en roles que permitan asignar diferentes niveles de permisos en la plataforma.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 28 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Acceso a las distintas funcionalidades e información de la plataforma basado en roles. Posibilidad de restringir el acceso a ciertas secciones de la herramienta a roles, usuarios o grupos de usuarios.

- El sistema a suministrar será en formato virtual compatible con la infraestructura virtual de la Consejería (Vmware) y no podrá tener limitaciones en cuanto al espacio en disco asignado a la máquina virtual.
- El centro de respuesta a incidentes de seguridad AndalucíaCERT se podrá integrar en este sistema para tareas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía. En concreto:
  - Se atenderán las solicitudes de acceso al sistema desde el CSIRT AndalucíaCERT, proporcionando usuarios de consulta.
  - Se atenderán las peticiones que lleguen desde AndalucíaCERT para duplicación y reenvío de tráfico, eventos y alertas a los sistemas de monitorización del CSIRT autonómico.

En cualquier caso este sistema, indistintamente de si es una solución de código abierto o un producto comercial, será instalado y configurado por parte del licitador, entregando una solución integrada en la infraestructura con las fuentes de eventos que decida la propia Consejería y de acuerdo a las características indicadas anteriormente.

Deberá ser completamente integrable con los sistemas ofertados en la presente licitación.

Este sistema podría darse conjuntamente con el de almacenado y sellado de logs.

5.3.7 Herramienta de análisis de vulnerabilidades

Las vulnerabilidades son una de las principales puertas de entrada para piratas informáticos, que están buscando constantemente nuevas formas de atacar cualquier sistema, servidor o red a través de estos fallos de seguridad, es por ello que se hace necesario analizar periódicamente los sistemas y aplicaciones en busca de fallos de seguridad para solucionarlos antes de que sea demasiado tarde.

Para ello se solicita una herramienta de análisis de vulnerabilidades que debe soportar, al menos, las siguientes características:

- La herramienta debe permitir realizar escaneos de vulnerabilidades contra un número ilimitado de direcciones IP.
- Detección de vulnerabilidades de sistemas y software, ausencia de parches de seguridad y configuraciones erróneas en sistemas operativos, dispositivos y aplicaciones.
- Detección de parámetros de certificados digitales.
- Informes configurables y personalizables.
- Soporte de más de 45000 CVEs
- Actualizaciones inmediatas, constantes y automáticas de firmas, CVEs y plugins.
- Análisis de contenedores.
- Exclusiones/excepciones de CVE en la configuración de los análisis.
- Exclusiones/excepciones de DDoS en la configuración de los análisis.
- Posibilidad de creación previa de plantillas para un uso más eficiente en análisis periódicos.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 29 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Auditoria WEB PCI.

- Planificación de análisis automáticos.
- Informes OWASP.
- Soporte para la instalación de la herramienta sobre sistemas operativos Microsoft Windows y Linux.

Para esta herramienta, se exigirá la instalación y configuración por parte del adjudicatario, en máquina virtual facilitada por la Consejería, bajo las políticas de instalación y puesta en producción que ésta determine.

5.4 Servicios y garantía técnica

Se incluirán todos los dispositivos y accesorios hardware y software (guías de armarios, cables, latiguillos, transceptores, controladores, interfaces, drivers, licencias, conexiones eléctricas, etc.) necesarios para el perfecto funcionamiento, instalación, puesta en producción y utilización de todos los elementos comprendidos en esta contratación. Serán por cuenta del adjudicatario, todos los gastos de transporte del suministro a los locales de instalación, así como los gastos de seguro y otros en que se incurriera para éste.

Se incluirán trabajos de migración que contemplarán no solo la configuración de la infraestructura actual durante la ejecución de las fases 0, 1 y 2, sino también posibles migraciones a, por ejemplo, sistemas o dominios virtuales que alberguen nuevos servicios provenientes de fases de consolidación de los sistemas de información existentes en múltiples CPDs de las diferentes Consejerías y organismos.

Las intervenciones de los técnicos, actualizaciones de equipos, conmutaciones de nodos o de tarjetas supervisoras, o cualquier cambio de configuración sobre la infraestructura en producción se efectuarán por personal del adjudicatario 'in situ', salvo que la Consejería acepte el trabajo remoto. Algunas de las intervenciones se realizarán fuera del horario habitual de trabajo (fines de semana, noches, etc), quedando a criterio de la Consejería la decisión del horario óptimo para cada intervención. Todos los gastos derivados de las intervenciones (desplazamientos, transportes de piezas o equipos, etc), serán por cuenta de la empresa adjudicataria, así como los gastos de desplazamiento de sus técnicos para la realización de las intervenciones requeridas, no pudiéndose reclamar abonos por estos conceptos.

En todos los casos, quedan incluidos dentro de los servicios los siguientes conceptos:

- Desplazamiento de los técnicos del adjudicatario al lugar de ubicación del equipo afectado.
- Mano de obra y servicios correspondientes.
- Equipamiento y herramientas (tanto hardware como software) necesarias para el correcto desempeño de las labores de soporte y mantenimiento exigidas por el presente contrato.
- Todos los materiales y componentes requeridos. Para ello el adjudicatario deberá garantizar la existencia de un stock suficiente de piezas y recambios para asegurar la reparación de los equipos
- Cualquier otro elemento que forme parte de la solución desplegada.

El adjudicatario gestionará la obtención para cada fabricante de cuentas de cliente que faciliten conocer el estado del soporte de todos los elementos ofertados y realizar el seguimiento de las incidencias y casos escalados a los fabricantes.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 30 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

5.4.1 Servicios de mantenimiento y soporte correctivo

Todos los elementos incluidos en este expediente (tanto hardware, como software, como servicios) deben estar cubiertos por el servicio de mantenimiento y soporte durante un periodo de mínimo 52 MESES a contar a partir de la fecha de puesta en producción del último de los mismos. La fecha de finalización será la misma para todos los sistemas y dependerá por tanto de la fecha de puesta en producción del último sistema.

Durante la duración del servicio de mantenimiento y soporte, la reparación de la infraestructura será gratuita para la Consejería, con independencia de si la reparación se realiza durante la vigencia del contrato o posteriormente durante la garantía del mismo.

La documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo, se solicitará su repetición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

El soporte y mantenimiento correctivo tiene como misión actuar en caso de incidencias, averías o problemas, cumpliendo con los niveles de ANS (Acuerdos de Nivel de Servicio) siguientes:

- Para todos los elementos de la infraestructura en caso de duda de carácter técnico, funcional, ajustes y optimización de configuraciones, se podrán realizar consultas vía telemática (correo electrónico y/o web) de forma ilimitada al adjudicatario, que garantizará su resolución en un plazo máximo de 1 semana.
- Para las infraestructuras de cortafuegos de nueva generación y balanceo de carga, control de acceso de usuarios y seguridad en las aplicaciones web balanceadas:
  - Servicio de mantenimiento en régimen 24x7
  - El tiempo de respuesta debe ser inferior a 30 minutos.
  - El tiempo de respuesta presencial debe ser menor de 4 horas para incidentes o problemas críticos.
  - El incidente o problema debe estar solucionado en menos de 8 horas en caso de pérdida de servicio, 24 horas en caso de degradación de servicio, 72 horas en caso de otros incidentes críticos y 1 semana en el resto de incidentes.
  - La criticidad de los incidentes o problemas será establecida por la Consejería en la comunicación de los mismos, pudiendo ser modificada posteriormente, también por la Consejería, en función del impacto en los servicios.
  - Se debe mantener cubierta la reparación, con la eventual sustitución de piezas deterioradas por piezas originales, de cualquier avería o mal funcionamiento que pudieran producirse. La gestión de las autorizaciones de devolución de mercancía (RMAs) con el fabricante según ANS Next-Day (el equipo o componente deberá ser reemplazado al siguiente día natural del día de la solicitud de reemplazo). Las piezas o equipos sustituidos serán nuevos y originales del fabricante del equipo y de características iguales o superiores a las sustituidas sin coste.
- Para el resto de infraestructuras:
  - Servicio de mantenimiento en régimen 8x5
  - El tiempo de respuesta debe ser inferior a 30 minutos.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 31 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- El tiempo de respuesta presencial debe ser menor de 4 horas para incidentes o problemas críticos.
- El incidente o problema debe estar solucionado en menos de 8 horas en caso de pérdida de servicio, 24 horas en caso de degradación de servicio, 72 horas en caso de otros incidentes críticos y 1 semana en el resto de incidentes.
- La criticidad de los incidentes o problemas será establecida por la Consejería en la comunicación de los mismos, pudiendo ser modificada posteriormente, también por la Consejería, en función del impacto en los servicios.
- Se debe mantener cubierta la reparación, con la eventual sustitución de piezas deterioradas por piezas originales, de cualquier avería o mal funcionamiento que pudieran producirse. La gestión de las autorizaciones de devolución de mercancía (RMAs) con el fabricante según ANS Next-Business-Day (el equipo o componente deberá ser reemplazado al siguiente día laboral del día de la solicitud de reemplazo). Las piezas o equipos sustituidos serán nuevos y originales del fabricante del equipo y de características iguales o superiores a las sustituidas sin coste.

El soporte y mantenimiento correctivo debe tener las siguientes siguientes características:

- La empresa adjudicataria habilitará mecanismos por vía telefónica y electrónica (incluyendo como mínimo la comunicación vía correo electrónico) que permitan la recepción de consultas y la comunicación de incidencias en régimen de 24x7 y siempre con atención en castellano.
- Escalado y gestión con los diferentes fabricantes de los bugs y las incidencias en caso de que sea necesario.
- Sustituir un equipo por otro nuevo de la misma naturaleza y prestaciones iguales o superiores sin coste adicional, ante la imposibilidad de la reparación del primero (se entiende que la sustitución supondrá la instalación en el nuevo equipo físico de todos los equipos lógicos de base, de aplicación y datos existentes en el equipo físico sustituido, así como su periferia. Asimismo, todas las operaciones de traslado e instalación de los equipos afectados correrán por cuenta del adjudicatario).
- Acceso a los parches, nuevas releases y versiones de software y firmware, alertas de seguridad y bases de datos de conocimiento de los productos adquiridos.
- En aquellos casos en que algún equipo esté conectado con elementos de diferentes suministradores de servicios de mantenimiento, el adjudicatario deberá responder del normal funcionamiento de los componentes cuyo mantenimiento está a su cargo, debiendo demostrar fehacientemente que las incidencias que él estima imputables a otros suministradores son las causantes del mal funcionamiento de los equipos.
- El adjudicatario en cualquier caso garantizará al finalizar el contrato un perfecto estado del funcionamiento de las máquinas y equipos.
- También se realizará la actualización de software de equipos por parte del adjudicatario y sin coste adicional, en el caso de que sea necesario para la resolución de incidencias provocadas por el mal funcionamiento del software (bugs) y/o actualización por problemas de seguridad. Esta actualización la realizará el adjudicatario in-situ, salvo decisión distinta de la Consejería.
- En este servicio también estará incluida como mínimo dos veces al años actualizaciones del software de todo el equipamiento en caso de que la Consejería lo estime oportuno. Esta actualización la realizará el adjudicatario in-situ, salvo decisión distinta de la Consejería.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 32 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Toda tarea incluida en el mantenimiento correctivo que pueda provocar pérdida o degradación de servicio se realizará fuera del horario laboral de la Consejería, o en cualquier caso en el horario 24x7 indicado por el Director del Proyecto.
- En el caso en que el adjudicatario tuviese dificultades para prestar el servicio en la forma y el tiempo estipulados, asumirá los gastos de facturación que se deriven al solicitar la prestación de estos servicios a otro proveedor incluido el fabricante de dichos equipos sin coste alguno para la Consejería.
- Todas las tareas incluidas, deben ser ejecutadas por personas certificadas por el fabricante del sistema implicado.
- Para cada incidencia o actuación realizada en la infraestructura, el adjudicatario deberá entregar en el plazo de siete días desde la resolución de la incidencia un informe detallado que recoja, al menos, la causa de la incidencia, su acotación en el tiempo, la solución aplicada y las acciones previstas realizar para evitar que se reproduzca en el futuro.
- Adicionalmente, el adjudicatario realizará informes periódicos, cada mes y bajo demanda a solicitud de la dirección del proyecto, como mínimo, con la información del estado de cada uno de los elementos de la infraestructura y de la capacidad de los mismos. El documento tiene como objetivo presentar el análisis de información realizado sobre los datos recogidos en la infraestructura ofertada. En el mismo se incluirán datos de inventario, análisis de rendimiento y capacidad de cada sistema, consumo de licencias. Adicionalmente se incluirá una comparación con los informes anteriores con la finalidad de ver la evolución y la utilización de los recursos de cada uno de los sistemas, así como proponer recomendaciones y mejores prácticas a aplicar sobre la plataforma, indicando posibles bugs/vulnerabilidades de las versiones instaladas en cada sistema. Este documento se utilizará como base para la comparativa periódica de capacidad de la infraestructura instalada y utilización de los recursos de infraestructura de Junta de Andalucía. Estos informes mensuales se presentarán antes del día 10 de cada mes y los solicitados a demanda en un plazo máximo de 7 días laborables. Al menos deberán incluir los siguientes indicadores:
  - Cortafuegos/IPS:
    - Número de objetos definidos, políticas de cortafuegos, NAT, descifrado SSL, políticas con un "ANY", con dos "ANY", sin perfiles de seguridad asociados, políticas sin uso en los últimos 6 meses. Bloqueos de conexiones con el IPS. Fecha de última actualización de firmas de IPS/antivirus. Consumos de CPU/memoria, sesiones concurrentes, consumos por interfaz de red. Cambios sustanciales respecto al informe anterior
  - ADC/WAF:
    - Número de servicios virtuales/nodos activos/deshabilitados, objetos sin usar, servicios securizados con WAF, firmas aplicadas por cada política, bloqueos de conexiones en el WAF. Fecha de última actualización de firmas. Consumos de CPU/memoria, sesiones concurrentes, consumos por interfaz de red, cambios sustanciales respecto al informe anterior
  - Proxy:
    - Número de políticas, usuarios concurrentes, usuarios con permisos especiales, cortes contra URLs de categorías maliciosas, cortes contra URLs de categorías prohibidas. Consumos de CPU/memoria, sesiones concurrentes, consumos por interfaz de red. Cambios sustanciales respecto al informe anterior.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 33 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

El servicio de mantenimiento estará cubierto por contratos de mantenimiento con el fabricante en España y la Consejería dispondrá de acceso a las páginas de soporte del fabricante para poder realizar el seguimiento de los casos de soporte abiertos y para la verificación del soporte contratado para cada elemento hardware y software de la infraestructura suministrada, incluyendo información de número de serie de los equipos, fecha inicio y fecha fin de soporte.

En caso que alguno de los sistemas de la infraestructura ofertada entre en el período de "end of life" (EOL), el adjudicatario estará obligado a sustituir dicho sistema por otro con rendimiento y funcionalidades iguales o superiores. En este caso, el proceso de instalación, configuración y migración será por parte del adjudicatario.

En caso de incumplimiento de las ANS acordados, se aplicarán las penalizaciones especificadas en el PCAP.

5.4.2 Servicio de soporte avanzado

Estos servicios, que se desarrollan a continuación, consisten en:

- Consultoría sobre nuevas tecnologías de seguridad de la información
- Servicio de monitorización de eventos de seguridad
- Pruebas de contingencia

La documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo, se solicitará su reedición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

5.4.2.1 Consultoría sobre nuevas tecnologías de seguridad de la información

Durante la ejecución del contrato, el adjudicatario deberá realizar una consultoría sobre las nuevas tecnologías de seguridad de la información, cuyo objetivo final es proporcionar conocimiento técnico a la Consejería acerca de la evolución de la arquitectura actual del infraestructura de seguridad perimetral a las nuevas posibilidades que ofrezca el panorama tecnológico en dicho momento. Esta consultoría deberá incluir distintas posibilidades tecnologías de distintos fabricantes.

Los licitadores incluirán en su oferta técnica una propuesta de consultoría en esta línea. La propuesta deberá comprender al menos una formación inicial de 6 horas sobre la materia, la elaboración de una propuesta de rediseño de la infraestructura actual mediante el uso de nuevas tecnologías, información sobre opciones de migración de la solución tecnológica que tenga la Consejería a estas otras soluciones tecnológicas, incluyendo su valoración económica y una sesión de al menos 6 horas para la presentación detallada de dicha propuesta.

Las tareas de consultoría se han estimado en 120 horas. No obstante, se deben cumplir los objetivos de estas tareas, especificadas anteriormente. Este servicio no consume horas de ninguna de las bolsas que se especifican más adelante.

5.4.2.2 Servicio de monitorización de eventos de seguridad

Mediante este servicio, el adjudicatario realizará informes periódicos, cada mes, como mínimo, con la información del sistema de gestión de eventos de seguridad, con al menos la siguiente información:

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 34 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Incidentes críticos abiertos.
- Incidentes pendientes.
- Incidentes creados según prioridad.
- Evolución de los incidentes.
- Recomendaciones a seguir para la resolución de los nuevos incidentes críticos abiertos.
- Información de seguimiento de la resolución de incidentes críticos del informe anterior.
- Recomendaciones de configuración de nuevas reglas de generación de eventos de seguridad y nuevas reglas de correlación.

5.4.2.3 Realización de pruebas de contingencia

Como parte de la comprobación efectiva del funcionamiento e implantación de la infraestructura según los criterios acordados, se realizará por parte del licitador las correspondientes pruebas de contingencia de cada sistema y de los cpd completos, previa generación de la correspondiente documentación detallada, de forma periódica, al menos una vez al año, teniendo en cuenta los escenarios indicados en el apartado "5.2.3 Arquitectura".

5.4.3 Servicios de valor añadido

Estos servicios, que se desarrollan a continuación, consisten en:

- Servicio de auditoría y certificación de sistemas de información de la CHIE.
- Bolsa de horas de asistencia técnica.
- Bolsa de horas de auditorias.
- Bolsa de horas de formación.

Los servicios y trabajos encuadrados fuera del presente apartado (Servicio de Valor Añadido), NO consumirán horas de las bolsas descritas a continuación.

Los servicios incluidos podrán ser realizados in-situ o en remoto y fuera de horario laboral en caso de que puedan provocar perdidas o degradación de servicio, según indicaciones del Director del Proyecto.

Las horas incluidas en los siguientes apartados podrán ser intercambiables entre ellas, según las necesidades del proyecto.

De manera genérica la solicitud de estos servicios de valor añadido se formalizará mediante correo electrónico del director de proyecto por parte de la Consejería al responsable del adjudicatario. Dicho correo contendrá al menos una descripción y alcance de los trabajos solicitados. Una vez aclaradas las dudas y/o consultas por parte del adjudicatario, deberá presentar una planificación y estimación de consumo de la bolsa de horas para la realización de dichos trabajos en un plazo máximo de 1 semana.

Una vez la dirección del proyecto valide la planificación y autorice los trabajos, el adjudicatario dispondrá como máximo de 2 semanas para el inicio de los mismos, salvo que se acuerde entre ambas partes un inicio concreto por necesidades del servicio.

Se deberán entregar en el plazo de siete días desde la finalización de las tareas solicitadas, un informe detallado de las mismas.

La documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo,

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 35 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

se solicitará su reedición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

5.4.3.1 Servicio de auditoría y certificación de sistemas de información de la CHIE

El Esquema Nacional de Seguridad (ENS) fue regulado inicialmente por el Real Decreto 3/2010, de 8 de enero. Posteriormente determinados puntos del ENS han sido actualizados en el Real Decreto 951/2015, de 23 de octubre, de modificación del Esquema Nacional de Seguridad. La Guía de Seguridad "CCN-STIC-809 – Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento" establece la necesidad, para aquellas entidades sujetas al ENS con sistemas de Nivel Medio o Alto, de obtener la Certificación del ENS.

Más recientemente ha sido aprobado el 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. Este Reglamento establece también requisitos de certificación en relación al tratamiento de datos. Es aplicable desde el 25 de mayo de 2018.

El 6 de diciembre de 2018 entró en vigor la nueva Ley orgánica de protección de datos y garantía de derechos digitales (LOPDGDD) que adapta al contexto español el RGPD europeo que había entrado en funcionamiento el 25 de mayo de 2018.

El adjudicatario deberá prestar un servicio de auditoría y de certificación de sistemas de información respecto del cumplimiento del ENS y de protección de datos (Reglamento UE 2016/679 y LOPDGDD), con las siguientes características:

- El adjudicatario prestará al menos 480 horas (60 jornadas) de servicios de "auditoría y certificación" de este tipo. Este servicio se aplicará a los servicios de la Junta de Andalucía y a uno de los dos bloques normativos citados (ENS y/o protección de datos (Reglamento UE 2016/679/LOPDGDD)). El servicio también podrá aplicarse a ambas normativas conjuntamente, consumiendo en este caso dos de las unidades de servicio ofertadas.
- Los servicios a auditar y certificar serán sistemas productivos de la Junta de Andalucía como GIRO, SIRHUS, SUR, Correo Corporativo, GUIA, Carpeta Ciudadana, etc.
- La decisión de qué sistemas tratar corresponderá al Director del Proyecto de la CHIE.
- Se requiere no solo la auditoría sino también la certificación del sistema respecto de la normativa a la que se aplique el servicio (ENS y/o Reglamento UE 2016/679/LOPDGDD).
- Las certificaciones con las que cuenta actualmente la Consejería son publicas y accesibles mediante la siguiente dirección: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/sector-public:
  - Los sistemas de información gestionados por la Dirección General de Transformación Digital de la Consejería de Hacienda, Industria y Energía, que dan soporte a la Junta de Andalucía en lo que se refiere a:
    - Gestión presupuestaria, contable y tesorera;
    - Gestión tributaria y de ingresos públicos;
    - Gestión de la contratación administrativa;

    así como otros componentes auxiliares para el funcionamiento de las plataformas principales, conforme a los requisitos de seguridad establecidos en el Real Decreto 3/2010, de acuerdo con la declaración de aplicabilidad vigente.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 36 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Los sistemas de información gestionados por la Dirección General de Transformación Digital de la Consejería de Hacienda, Industria y Energía, que dan soporte a la Junta de Andalucía en lo que se refiere a:
  - Gestión de la función pública;

  Conforme a los requisitos de seguridad establecidos en el Real Decreto 3/2010, de acuerdo con la declaración de aplicabilidad vigente
- Los sistemas de información gestionados por la Dirección General de Transformación Digital de la Consejería de Hacienda, Industria y Energía, que dan soporte a la Junta de Andalucía en lo que se refiere a:
  - Administración electrónica, incluyendo el registro electrónico único, la ventanilla electrónica, la firma electrónica, el sellado de tiempo y el sistema de notificaciones telemáticas;
- Conforme a los requisitos de seguridad establecidos en el Real Decreto 3/2010, de acuerdo con la declaración de aplicabilidad vigente

- El objetivo de este servicio es el obtener certificaciones de los sistemas de la Consejería en las mismas condiciones que las certificaciones actuales indicadas en el punto anterior.
- También se podrán solicitar la recertificación de alguno de los servicios de la Junta de Andalucía que ya cuenten con una certificación anterior caducada o próxima a caducar.
- Como referencia, las certificaciones indicadas anteriormente, se realizaron en 15 jornadas.
- La certificación podrá obtenerse de dos maneras:
  - Directamente en caso de que en la auditoría no se detecten disconformidades.
  - Con posterioridad a la auditoría en caso de que se detecten disconformidades y estas sean resueltas por la Consejería antes de la finalización del contrato. El informe de auditoría deberá dejar claras por tanto las posibles disconformidades y plantear las medidas concretas a adoptar para subsanarlas.
- La certificación deberá ser emitida por entidades de certificación acreditadas para tal finalidad. En este sentido:
  - La acreditación de entidades de certificación respecto del ENS corresponde a la Entidad Nacional de Acreditación (ENAC). Por tanto la certificación respecto del ENS deberá ser emitida por una entidad certificadora acreditada para esta finalidad por ENAC.
  - La acreditación de entidades de certificación respecto del Reglamento UE 2016/679 está regulada por el artículo 43 del citado Reglamento. Por tanto la certificación respecto del Reglamento UE 2016/679 deberá ser emitida por una entidad certificadora acreditada para esta finalidad en los términos previstos en el propio Reglamento.
- Dado que el Reglamento UE 2016/679 tiene carácter europeo es posible que surjan entidades certificadoras en los distintos estados miembros, siendo válida cualquier entidad certificadora del Reglamento UE 2016/679 en tanto cumpla los requisitos legales. Sin embargo, el idioma de trabajo para reuniones, comunicaciones y documentación en relación con este servicio será el español.
- Como resultado de cada servicio de auditoría y certificación, el adjudicatario deberá facilitar los siguientes entregables, que estarán sujetos a la aprobación del Director del Proyecto:
  - Informe de auditoría
  - Certificación oficial de cumplimento, con el ENS y/o protección de datos (Reglamento UE 2016/679/LOPDGDD)

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 37 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

5.4.3.2 Bolsa de horas de asistencia técnica

Este servicio se regulará mediante una bolsa de horas de asistencia in-situ, con las siguientes características:

- La bolsa de horas incluirá un mínimo de 300 horas
- Al tratarse de asistencia in-situ no consumirán horas los desplazamientos.
- En el marco de esta bolsa se realizarán actividades de apoyo, ajuste y optimización de la solución ofertada una vez puesta en marcha.
- Dado que en el ámbito de la Ciberseguridad es prácticamente imposible definir con absoluta precisión el alcance y límites de todos los servicios de seguridad que se puedan requerir durante el periodo de ejecución del contrato, considerando que la tecnología evoluciona y cambia día a día, los ataques se profesionalizan y las TIC están ya presentes en todos los ámbitos de competencia de la Administración de la Junta de Andalucía. Así, se contempla la posibilidad de incorporación, durante la vigencia del contrato, de servicios adicionales de seguridad, que en el caso de necesidad, se incluirán a través de esta bolsa de horas.
- Estas actividades se realizarán bajo petición de la Consejería.
- Toda tarea incluida que pueda provocar pérdida de servicio, se realizará fuera del horario laboral de la Consejería.

5.4.3.3 Bolsa de horas de auditoría

Este servicio se regulará mediante una bolsa de horas de auditorias, con las siguientes características:

- La bolsa de horas incluirá un mínimo de 500 horas
- Este servicio se regulará mediante una bolsa de auditorías de seguridad y hacking ético tanto in-situ como en remoto, pudiendo ser tanto auditorías de caja negra, como de caja blanca.
- En el caso de trabajos in-situ, no consumirán horas los desplazamientos.
- Las auditorías no deben limitarse al uso de herramientas automatizadas.
- Se realizarán auditorías sobre la solución instalada para la realización análisis de riesgos, test de rendimiento, test de intrusiones y demás test que se soliciten por parte de la Consejería para comprobar el estado y buen funcionamiento de la solución instalada.
- También auditorías sobre otros sistemas de información de la Consejería que designe el Director de Proyecto, realizadas tanto desde Internet como desde la Red Corporativa de la Junta de Andalucía (RCJA), para la detección de:
  - Vulnerabilidades del sistema soporte de la aplicación.
  - Vulnerabilidades que permitan la ejecución de código remoto por incorrecta validación de datos.
  - Vulnerabilidades relacionadas con la autenticación, autorización y gestión de sesiones.
  - Vulnerabilidades derivadas de configuraciones erróneas de seguridad o inadecuada actualización de componentes.
  - Vulnerabilidades derivadas de empleo de métodos criptográficos débiles.
  - Vulnerabilidades derivadas de incorrecta gestión de errores y logs de eventos de la aplicación.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 38 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Realización de Auditorías de Seguridad basadas en fuentes abiertas (OSINT), detectando los posibles fallos de seguridad y gestionando las vulnerabilidades descubiertas.
- Estas actividades se realizarán bajo petición de la Consejería.
- Toda tarea incluida que pueda provocar pérdida de servicio, se realizará fuera del horario laboral de la Consejería.

El adjudicatario elaborará un informe de resultados en cada revisión, donde se describa el alcance, las pruebas realizadas y los resultados obtenidos, categorizados en base a niveles de riesgo e impacto para el servicio.

Los licitadores deberán indicar, en su oferta técnica, el equipo técnico de seguridad que pondrán a disposición de este servicio, así como la metodología de análisis que aplicará, áreas de seguridad a analizar y técnicas y herramientas de explotación de vulnerabilidades utilizadas.

Los análisis manuales de seguridad se realizarán habitualmente en el entorno de producción estando obligado el adjudicatario a asegurar que las actividades no comprometan la integridad de los datos objeto de revisión, la disponibilidad del servicio analizado ni otros servicios ajenos a la aplicación en revisión. De igual forma, por tratarse de aplicaciones en producción, las ventanas horarias de trabajo deberán ser acordadas entre la Consejería y el adjudicatario, normalmente fuera del horario de producción, para asegurar el mínimo impacto en el servicio analizado.

5.4.3.4 Bolsa de horas de formación

Este servicio se regulará mediante una bolsa de horas de formación in-situ, con las siguientes características:

- La bolsa de horas incluirá un mínimo de 200 horas
- No se contabilizan los posibles desplazamientos, así como las posibles horas necesarias para la preparación del curso por parte del profesor.
- Se realizarán cursos con temario a definir por la Consejería relacionados con la seguridad en la nube, seguridad en devops, seguridad en el desarrollo de software, y otros temas de seguridad de la información e infraestructuras TIC, ya que dado que en el ámbito de la Ciberseguridad es prácticamente imposible definir con absoluta precisión el alcance y límites de la formación, considerando que la tecnología evoluciona y cambia día a día, los ataques se profesionalizan y las TIC están ya presentes en todos los ámbitos de competencia de la Administración de la Junta de Andalucía.
- Se impartirán en las instalaciones de la Consejería y en el horario que indique el Director del Proyecto.
- Mínimo de 20 participantes.
- Se incluirán en la oferta sugerencias de temario para posibles cursos de formación aunque la temática de los cursos será decisión del Director de Proyecto.

5.4.4 Servicios de capacitación técnica y transferencia de conocimiento

Se incluirá un plan de formación elaborado e impartido por cuenta del adjudicatario referente al entrenamiento y capacitación necesaria para que el personal de la Junta de Andalucía obtenga los conocimientos necesarios para la utilización y operación de todos los elementos hardware y software propuestos adecuándose al nivel de conocimientos previos sobre las tecnologías que ya disponga el

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 39 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

personal de la Junta de Andalucía. Este servicio es independiente de la bolsa de horas de formación descrita anteriormente y no consume horas, por tanto, de la misma.

Se establecen tres conceptos de formación:

- Transferencia de conocimientos inicial (incluida en Fase 0).
- Formación a medida (incluida en Fase 1 y 2).
- Transferencia de conocimientos sobre la infraestructura ya implantada (incluida en Fase 2).
- Otras formaciones adicionales (incluida en Fase 3).

La transferencia de conocimientos inicial está orientada a la descripción detallada de la infraestructura ofertada y de la propuesta de implantación por parte del adjudicatario.

El contenido de los cursos de formación a medida deberá coincidir con el de los cursos de formación reglada del correspondiente fabricante, y deberá ser impartida con personal adecuadamente formado y certificado en el fabricante.

La transferencia de conocimientos sobre la infraestructura ya implantada está orientada a la descripción detallada de la implantación y configuraciones realizadas, de la integración entre componentes y de la utilización, mecanismos de funcionamiento y dependencias de los mismos.

Las formación adicional contará con una serie de cursos relacionados con temas de seguridad de la información y cuya temática y propuesta de temario se describirán mas adelante.

El plan de formación debe incluir, al menos, una edición de todos los cursos. Todas las sesiones de formación estarán dimensionadas para al menos 20 personas. Deben incluirse los siguientes conceptos:

- Transferencia de conocimientos inicial:
  - Deberán realizarse al menos una sesión para la descripción detallada de la infraestructura ofertada y de la propuesta de implantación, que a la vez podría servir como toma de requisitos por parte del adjudicatario, para la realización de la configuración final de todos los sistemas ofertados. El contenido de esta sesión no se limitará a la enumeración y descripción de la oferta, sino que se deberá describir de forma detallada la propuesta de implantación acordada tras haber mantenido las primeras reuniones del proyecto.
  - La duración de cada sesión se adaptará al contenido de la misma, con un mínimo de cinco jornadas (32 horas lectivas).
  - Se impartirán en las instalaciones de la Consejería y en el horario que indique el Director del Proyecto.
  - Como mínimo deberá incluir los contenidos solicitados por el Director del Proyecto de la Consejería y que a modo orientativo deberán cumplir:
    - Arquitectura propuesta.
    - Descripción del funcionamiento y utilización de todos los componentes de la solución (tanto hardware como software).
    - Licenciamiento ofertado.
    - Interdependencias.
    - Opciones de diseño y puesta en marcha.
    - Procedimiento de migración propuesto.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 40 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Formación a medida:
  - El contenido de los cursos de formación a medida deberá coincidir con el de los cursos de formación reglada del correspondiente fabricante, y deberá ser impartida con personal adecuadamente formado y certificado en el fabricante.
  - Habrá una sesión de formación por cada plataforma incluida en la oferta y la duración de cada sesión de formación se adaptará al contenido de la misma, con un mínimo de cinco jornadas (32 horas lectivas).
  - Se impartirán en las instalaciones de la Consejería y en el horario que indique el Director del Proyecto.
  - A modo de orientación, el temario para cada uno de los sistemas/funcionalidades incluidas en la oferta, incluirá al menos los siguientes puntos:
    - Descripción del hardware
    - Descripción del software
    - Configuración inicial y puesta en marcha del sistema
    - Activación de licencias
    - Configuración del cluster
    - Configuración de la autenticación
    - Configuración de la red
    - Configuración de todas las funcionalidades disponibles en el sistema. Por ejemplo para la infraestructura de cortafuegos:
      - Configuración de routing
      - Configuracion de políticas de seguridad
      - Configuración de filtrado de contenidos
      - Configuración de perfiles de seguridad
      - Configuración de la identificación de usuarios
      - Configuración de QoS
    - Configuración de la monitorización propia del sistema
    - Configuración e integración con elementos de monitorización externa
    - Configuración y generación de reportes
    - Troubleshooting
- Transferencia de conocimientos final:
  - Antes de la realización de esta sesión de transferencia de conocimiento, deberá estar finalizada la implantación y puesta en producción de todos los elementos de la oferta, entregada y prevalidada por parte del Director del Proyecto toda la documentación entregable correspondiente a las fases de análisis/implantación/migración/puesta en producción. La validación definitiva de toda la documentación se realizará tras las sesiones de transferencia de conocimientos.
  - Deberá realizarse al menos una sesión.
  - La duración de cada sesión se adaptará al contenido de la misma, con un mínimo de quince jornadas (90 horas lectivas).
  - Se impartirán en las instalaciones de la Consejería y en el horario que indique el Director del Proyecto.
  - Como mínimo deberá incluir los contenidos solicitados por el Director del Proyecto de la Consejería y que a modo orientativo deberán cumplir:

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 41 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

        - Arquitectura implantada.
    - Configuración realizada.
    - Descripción del funcionamiento y utilización de todos los componentes de la solución (tanto hardware como software).
    - Interdependencias.
    - Motorización y gestión de alarmas/incidencias.
    - Explicar detalladamente todas las tareas de mantenimiento requeridas por la infraestructura desplegada.
    - Procedimientos de determinación de problemas de la infraestructura desplegada.
    - Procedimiento de migración empleado. Resultados de la migración.
    - Resumen ejecutivo.
- Otras formaciones adicionales:
  - Gestión de Ciberriesgos y Ciberseguros: esta formación responde a la situación actual en la que crece la demanda de ciberseguros, ya que las soluciones que solo contemplan la prevención no son eficaces y la seguridad absoluta es imposible. Lo que se puede hacer es establecer mecanismos de mitigación para disminuir el impacto de esos ataques en cuanto se produzcan, siendo una solución eficaz es la contratación de un ciberseguro.

    Temario orientativo:
    - Visión actual del ciberriesgo
    - Identificación de los ciberriesgos
    - Ciberseguridad: Gobierno de la seguridad, Gestión del riesgo, Políticas de seguridad, Política de salvaguardas, Planes de contigencias
    - Partes y peritaciones.
    - Cibercrimen: Exploits Kits, Botnets, Troyanos, Malware avanzado, Ransomware, APT's
    - Aspectos legales de la ciberseguridad
    - Evitar, aceptar, mitigar o transferencias de los ciberriesgos (ciberseguros)
    - Aspectos legales de la respuesta a incidentes
    - Informática forense en ciberseguros
    - Inteligencia en fuentes abiertas en ciberseguros
    - Reputación digital. Comunicación de crisis. Partes
    - Fraude y gestión de la identidad online
    - Derecho informático y de las TIC's
    - Derecho procesal y derechos humanos en el ciberespacio
    - Responsabilidad penal de las personas jurídicas
    - Ciberseguridad industrial (IT/OT)
    - Jurisprudecia en ciberseguros
    - Calculo de valor asegurado en ciberseguros
    - Aseguramiento
    - Recomendaciones para tasaciones, peritaciones y apertura de partes.
    - Casos prácticos
      - Redacción de pólizas de ciberseguros
      - Peritajes en ciberseguros
      - Contratos de ciberseguros

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 42 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Formación y certificación de Delegado de Protección de Datos: el Delegado de Protección de Datos (DPD o DPO en inglés), es una figura recogida en la sección 4 del capítulo IV del 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 y a la libre circulación de esos datos.
  Para conseguir la certificación como Delegado de Protección de Datos, se deben superar un proceso de 2 fases:
  - Prerrequisitos. Existen 4 vías para superar esta fase:
    - Candidatos que justifiquen una experiencia profesional de, al menos, 5 años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos
    - Candidatos que justifiquen una experiencia profesional de, al menos, 3 años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos y una formación reconocida de 60 horas en relación con las materias del esquema
    - Candidatos que justifiquen una experiencia profesional de, al menos, 2 años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos y una formación reconocida de 100 horas en relación con las materias del esquema
    - Candidatos que no cuenten con experiencia profesional y que tengan una formación reconocida de 180 horas en relación con las materias del esquema
  - Examen: el adjudicatario deberá incluir en la oferta formación y derechos para presentarse a examen para al menos 8 personas. Dicha formación deberá poder ser de hasta 180 horas, dado el peor de los casos de que las personas designadas a conseguir la certificación no tengan experiencia profesional, o la necesaria según la experiencia justificada. Debe ser impartida por un Centro de Formación Reconocido acreditado por una Entidad de Certificación para la figura del Delegado de Protección de Datos. La formación y el examen deberá ser en instalaciones de la Junta de Andalucía en Sevilla y en el horario que designe el Director del Proyecto.
- Certified SOC Analyst (CSA) de Eccouncil: el adjudicatario deberá incluir en la oferta formación para al menos 20 personas y derechos para presentarse a examen para al menos 8 personas. La formación y el examen deberá ser en castellano y en las instalaciones de la Junta de Andalucía en Sevilla y en el horario que designe el Director del Proyecto.
- Actualización normativa ENS: el adjudicatario deberá incluir en la oferta una formación de mínimo 20 horas sobre las actualizaciones de la normativa del ENS. Esta formación se realizará a petición del Director del Proyecto a lo largo de la ejecución del contrato y en caso de no realizarse, las horas pasarán a formar parte de la bolsa de horas de formación. Deberá ser en castellano y en las instalaciones de la Junta de Andalucía en Sevilla y en el horario que designe el Director del Proyecto.
- Actualización normativa de protección de datos: el adjudicatario deberá incluir en la oferta una formación de mínimo 20 horas sobre las actualizaciones de la normativa sobre la protección de datos. Esta formación se realizará a petición del Director del Proyecto a lo largo de la ejecución del contrato y en caso de no realizarse, las horas pasarán a formar parte de la bolsa de horas de formación. Deberá ser en castellano y en las instalaciones de la Junta de Andalucía en Sevilla y en el horario que designe el Director del Proyecto.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 43 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

La formación (ya sea a medida, transferencia de conocimiento o formación adicional) irá dirigida a personal técnico informático de la Junta de Andalucía que designe el Director de Proyecto, en número y perfil adecuado a la naturaleza de los productos y al contenido de los correspondientes cursos o actividad de formación.

Se espera una formación de calidad (en todas las modalidades) acorde a la complejidad de la tecnología de la solución adquirida y, por tanto, en caso de que la formación no se realice con unos mínimos de calidad razonables, se podrá solicitar por parte de la Consejería una reedición de dicha formación sin coste alguno añadido.

Además, toda la documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo, se solicitará su reedición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

De manera genérica la solicitud de estos servicios se formalizará mediante correo electrónico del director de proyecto por parte de la Consejería al responsable del adjudicatario. Una vez aclaradas las dudas y/o consultas por parte del adjudicatario, deberá presentar una planificación para la realización de dichos trabajos en un plazo máximo de 1 semana.

Una vez la dirección del proyecto valide la planificación y autorice los trabajos, el adjudicatario dispondrá como máximo de 1 mes para el inicio de los mismos, salvo que se acuerde entre ambas partes un inicio concreto por necesidades del servicio.

Con una antelación de al menos una semana respecto del inicio de la impartición de cada curso de formación, el adjudicatario proporcionará el temario y el contenido y documentación del mismo en formato papel y en formato electrónico estandarizado (pdf y editable en formato OpenDocument) a la Dirección de Proyecto.

Se impartirán en castellano, en las instalaciones de la Consejería y en el horario que determine el Director del Proyecto.

No computarán como horas lectivas los eventuales descansos para comer. Las horas de preparación de los cursos no computarán como horas lectivas ni consumirán horas de las bolsas de servicios de valor añadido.

Se deberán emitir certificados de aprovechamiento de la formación impartida a nombre de los asistentes a cada curso de formación, siguiendo el modelo de certificado que proporcionará el Director de Proyecto al adjudicatario. Los certificados deberán ir firmados por la persona física que tenga el cargo de responsable de la empresa adjudicataria del contrato. A decisión de la Consejería, también se podría admitir la firma de la persona física del responsable de la empresa de formación que se haya ocupado de impartir el curso, caso de que la empresa adjudicataria sea diferente a la empresa que imparte la formación.

Las sesiones de traspaso de conocimientos serán impartidas por los ingenieros encargados del diseño, configuración e implantación de la solución.

La formación a medida será impartida preferentemente por personal del fabricante de la solución y en todo caso el técnico encarga de impartir la formación deberá estar certificado oficialmente por el fabricante en la solución ofertada de la que es objeto la formación.

En el caso de cursos relativos a producto, el temario de cada sesión de formación deberá estar actualizado a la última versión de producto y a la funcionalidad del mismo.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 44 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

A partir de la relación de cursos adicionales indicados anteriormente, el Director del Proyecto indicará qué cursos se requieren y en qué momento de la ejecución del contrato deben impartirse.

El Director del Proyecto podrá requerir que no se imparta alguno de los cursos de formación anteriormente indicados y las horas asignadas a dicho curso pasara a la bolsa de horas de formación.

La empresa adjudicataria quedará a disposición de la Consejería, para asistir en dudas puntuales y aclaraciones que surjan respecto a la infraestructura instalada y su administración, durante los seis meses siguientes a la certificación de la finalización de la instalación y puesta en marcha.

En el plan de implantación deberán incluirse las horas de formación y los contenidos a desarrollar.

Materia	**Horas lectivas (mínimo)**	**Formadores**	**Asistentes (mínimo)**	**Observaciones**
Traspaso de conocimientos inicial	32h (5 jornadas)	La formación la impartirán los técnicos que vayan a realizar la puesta en marcha de cada sistema.	20	Formación inicial impartida por el adjudicatario al personal de la Junta de Andalucía sobre todo el hardware y software a instalar y los planes de implantación.
Sistema de cortafuegos NGFW	32h	Con certificación de fabricante.	20	Formación reglada completa (administración del sistema y todas sus funcionalidades)
Sistema de balanceo de carga, control de acceso de usuarios y seguridad en aplicaciones web balanceadas	32h	Con certificación de fabricante	20	Formación reglada completa (administración del sistema y todas sus funcionalidades)
Sistema de acceso seguro a Internet	32h	Con certificación de fabricante	20	Formación completa (administración del sistema y todas sus funcionalidades), que deberá ser reglada si se tratara de un software comercial.
Sistema de almacenado y sellado de logs	32h	Certificados por el fabricante en caso de ser un producto comercial. Con experiencia en la solución si fuera software libre.	20	Formación completa (administración del sistema y todas sus funcionalidades), que deberá ser reglada si se tratara de un software comercial.
Sistema de gestión de eventos de seguridad	32h	Certificados por el fabricante en caso de ser un producto comercial. Con experiencia en la solución si fuera software libre.	20	Formación completa (administración del sistema y todas sus funcionalidades), que deberá ser reglada si se tratara de un software comercial.
Análisis de vulnerabilidades	8h	Con certificación de fabricante	20	Formación reglada completa (administración de la herramienta y todas sus funcionalidades)

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 45 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Traspaso de conocimientos sobre la infraestructura instalada	90h (15 jornadas)	La formación la impartirán los técnicos que hayan realizado la puesta en marcha de cada sistema.	20	Formación adicional impartida por el adjudicatario al personal de la Consejería sobre todo el hardware y software instalado, las configuraciones realizadas en los diferentes sistemas, las generaciones de informes y operativas comunes para cada sistema.
Gestión de Ciberriesgos y Ciberseguros	32h		20	Temario orientativo
Delegado de Protección de Datos	180h	Centro de Formación Reconocido acreditado por una Entidad de Certificación para la figura del Delegado de Protección de Datos.	20 (8 derechos de examen)	Temario oficial
Certified SOC Analyst (CSA)	24h		20 (8 derechos de examen)	Temario oficial
Actualización normativa de protección de datos	20h		20	
Actualización normativa de protección de datos	20h		20	

5.4.5 Gestión de proyecto

Para la puesta en marcha de la infraestructura ofertada, así como para la migración de la infraestructura actual, se deberá presentar una programación detallada con los mínimos cortes de servicio posibles, por lo que el adjudicatario en todo momento estará en contacto con la Consejería, y en tal caso, solo se realizarán los trabajos en la fecha y rango horario determinados y autorizados por el Director del Proyecto de la Consejería (todos los trabajos que impliquen corte o degradación del servicio deberán realizarse en horario nocturno y/o fin de semana, sin coste adicional alguno, y siempre bajo la aprobación por el Director del Proyecto de la Consejería). Adicionalmente, si fuese necesario algún corte de servicio, se entregará, previo a la realización de los trabajos que produzcan dicho corte (y previa aprobación por el Director del Proyecto de la Consejería), un informe del mismo, que deberá incluir al menos:

- Plan detallado de los trabajos a realizar que provocan el corte de servicio.
- El horario propuesto y la duración estimada tanto de los trabajos a realizar como del corte de servicio, a la espera de la aprobación del Director del Proyecto de la Consejería.
- Para casos de necesidad, plan de restauración al punto inicial de partida antes de los trabajos a realizar. Duración estimada para la restauración del servicio y casos en los que pueda ser necesario la ejecución de este plan de restauración.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 46 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Recursos afectados.
- Personal que acudirá a la realización de los trabajos.

Junto con la oferta deberá incluirse una planificación detallada en el tiempo con indicación de las tareas, los recursos humanos y los materiales necesarios que hagan posible el éxito a plena satisfacción del presente Pliego.

Todos los elementos de la instalación irán debidamente identificados. Se entregará documentación técnica completa y preferentemente en castellano de los sistemas que se proporcionen, en formato electrónico y adicionalmente en formato papel.

Los trabajos de instalación e integración deberán ser realizados preferentemente por técnicos del fabricante de la infraestructura ofertada y en caso de que esto no fuera posible o tuviera una repercusión económica alta en la totalidad del proyecto, siempre sería realizada por técnicos de la empresa suministradora, certificados para estas labores por el fabricante al nivel adecuado, pero siempre bajo la aprobación por el Director del Proyecto de la Consejería.

La Consejería se reserva el derecho de exigir la documentación de capacitación exigida en el párrafo anterior, en el momento de la instalación, o la sustitución total o parcial de los técnicos encargados del trabajo antes o durante la realización del mismo.

Además, toda la documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo, se solicitará su reedición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

El adjudicatario establecerá un solo punto de contacto con la Consejería, y será responsable de registrar el progreso y poner al día al Director del Proyecto de la Consejería. El perfil del personal asignado para esta tarea se solicita en la documentación a entregar en el sobre 2. La asignación de este recurso por parte del licitador para esta gestión de proyecto, no consumirá horas de las bolsas descritas anteriormente.

Las peticiones para acceder a las áreas de acceso limitado o restringido del CPD de la Junta de Andalucía se realizarán al menos con un día laboral de antelación. La información crítica para la finalización de las tareas o del proyecto es un requerimiento que se comunicará al Director del Proyecto. La información ocasional se incluirá en los informes de progreso y seguimiento del proyecto que será elaborada por el adjudicatario.

El adjudicatario mantendrá la instalación de la Junta de Andalucía de forma ordenada y limpia. Las instalaciones de la Junta de Andalucía se mantendrán en condiciones óptimas de limpieza una vez finalizado el trabajo de cada día.

5.4.6 Plan de proyecto

El plan de implantación que las empresas licitadoras deben entregar como parte de la oferta será revisado y validado por el Director del Proyecto. Debe considerarse éste como un proyecto llave en mano, cuyo objetivo final es la implantación del nuevo sistema de forma que preste servicio a los sistemas y servicios TIC en producción, de forma que el proceso sea totalmente transparente para el usuario final.

Se debe desarrollar una propuesta técnica de migración, con la inclusión de un cronograma detallando tareas a realizar y el plan de migración de servicio, planes de pruebas y previsión de ventanas de corte de servicio.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 47 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Para una mayor legibilidad en la información a aportar, el licitador podrá estructurar las fases del proyecto que se indican en este apartado separadas en los distintos componentes que forman parte de la infraestructura. A modo de ejemplo, sería:

- Elementos que forman parte de la infraestructura ofertada
- Sistema de gestión de cada componente de la infraestructura ofertada
- Sistema de monitorización de la infraestructura ofertada. Integración del sistema de monitorización con el sistema de monitorización de la Junta de Andalucía.
- Cualquier otro componente necesario para la integración de la infraestructura ofertada con la infraestructura TIC de la Junta de Andalucía.

El plan de implantación abarcará los trabajos que a continuación se detallan. Si a lo largo de este proceso se detectase que falta algún elemento hardware o software para el óptimo funcionamiento de todos los procesos que se deben ejecutar en los equipos según las especificaciones de este pliego o las especificaciones indicadas en la oferta del adjudicatario, éste deberá ser suministrado e instalado por la empresa adjudicataria sin coste alguno ni menoscabo del resto del suministro, aun cuando no haya sido incluido en la oferta.

Los trabajos se estructurarán en fases, las cuales en algunos casos no podrán solaparse en el tiempo y en otros casos sí, según se defina en el plan de implantación.

Conviene resaltar la importancia de la puesta en marcha para el buen fin del proyecto, puesto que no solo se trata de instalar sistemas nuevos, sino de implantar sistemas y servicios TIC que se encuentran en producción y que no pueden ser detenidos arbitrariamente y por tiempo indeterminado. Por todo ello este proceso debe ser planificado con sumo cuidado y primando siempre que el impacto sobre los usuarios del sistema sea mínimo.

Además, toda la documentación, planificación e informes de este servicio deberán tener una calidad mínima aceptable que valorará la Dirección del Proyecto de la Consejería. En caso de no llegar a ese mínimo, se solicitará su reedición y constará como no entregado a efecto de indicadores de servicio y penalizaciones.

En resumen, el proceso de instalación, configuración y migración deberá cumplir tres requisitos indispensables: que se realice con absoluta continuidad (evitar tiempos muertos), que se realice en el menor plazo de tiempo posible (simultanear tareas) y que se minimice el tiempo de suspensión total del servicio.

Por otra parte, la empresa adjudicataria debe comprometerse (aparte de las condiciones de garantía) a que, desde el inicio hasta los dos meses siguientes a la finalización de la implantación de la infraestructura, existirá máxima disponibilidad de la misma para la resolución de cualquier problema que surja, de forma que se deberá proporcionar un tiempo de respuesta inferior a cuatro horas y se trabajará con continuidad hasta la resolución del mismo.

5.4.6.1 Fases de ejecución del proyecto

Se identifican las siguientes fases en el proyecto:

- **FASE 0: ANÁLISIS DE LA SITUACIÓN ACTUAL, CONSULTORÍA Y DISEÑO DE LA NUEVA SOLUCIÓN.** Análisis y consultoría de la infraestructura existente, así como el diseño de la implantación de la nueva infraestructura y de los planes para la migración de sistemas a la misma, incluyendo el diseño de la necesaria integración de la nueva infraestructura a suministrar con los sistemas de la Junta de Andalucía. En esta fase también se realizará la

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 48 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

transferencia de conocimientos inicial por parte del adjudicatario, la cual se especifica en el apartado de formación. Esta fase tendrá un periodo máximo de ejecución de 2 MESES. La toma de datos necesaria será realizada de manera íntegra por el adjudicatario.

Una vez finalizada esta fase, el adjudicatario deberá presentar un documento acreditativo de diseño la infraestructura acorde a las buenas prácticas recomendadas por el fabricante de la solución. Dicho documento deberá estar emitido, sellado y firmado por parte del fabricante de cada infraestructura.

- **FASE 1: SUMINISTRO, PUESTA EN FUNCIONAMIENTO DE LOS ELEMENTOS SUMINISTRADOS, COMPROBACIÓN DE LAS FUNCIONALIDADES ADQUIRIDAS Y VALIDACIÓN DE PLAN DE MIGRACIÓN**. Esta fase tendrá un periodo máximo de ejecución de 4 MESES desde la finalización de la fase anterior y comprenderá todas las siguientes tareas:
  1. El suministro de todos los elementos hardware y software ofertados y de todos los elementos hardware y software necesarios para la implementación de la solución propuesta. Todos los equipos y licencias se suministrarán en régimen de propiedad de la Junta de Andalucía. Dicho suministro puede realizarse en paralelo a la FASE 0.
  2. Instalación física de todos los equipos y de todos los componentes de cada uno de ellos sin excepción alguna y según las directrices del Director del Proyecto. El adjudicatario asegurará la plena operatividad del conjunto una vez instalado.
  3. Conexionado de todos los equipos.
  4. Etiquetado de los equipos y de todas las conexiones realizadas (sean nuevas o no), en ambos extremos de las conexiones. El formato y tipo de las etiquetas se realizará conforme a las indicaciones del Director del Proyecto.
  5. Instalación y configuración de todo el hardware y software para que funcione correctamente según las especificaciones de este pliego y las directrices del Director del Proyecto. Se deberán instalar o activar todas las funcionalidades ofertadas. Se deberán seguir en la medida de lo posible las configuraciones incluidas en las guiás del CCN-CERT.
  6. Definición y entrega del procedimiento a seguir para la migración de los servicios desde sus ubicaciones actuales a los nuevos sistemas. La Consejería deberá validar este plan con anterioridad a empezar la FASE 2.
  7. Comprobación de las funcionalidades adquiridas, pruebas y validación del plan de migración desarrollado en la FASE 0.

  La instalación del equipamiento incluirá los cables de alimentación con el conector acorde a las PDU existentes en los armarios, los materiales necesarios para la instalación en armario estándar de 19", los conectores y latiguillos de fibra y cobre necesarios para la interconexión de todos los equipos suministrados y todo material adicional y trabajos necesarios para la completa implantación de la solución propuesta e integración con el resto de infraestructura de la Junta de Andalucía en los distintos CPDs.

  En esta fase se podrá realizar, a decisión por parte de la Consejería, la prueba de concepto citada con anterioridad en el presente pliego.

- **FASE 2: EJECUCIÓN DE PLAN DE MIGRACIÓN Y PUESTA EN PRODUCCIÓN.** Esta fase tendrá un periodo máximo de ejecución de 2 MESES, comenzará después del final de la FASE 1 y contendrá todas las tareas de la ejecución del plan de migración desarrollado en la

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 49 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

FASE 0 y validado en la FASE 1, la integración de la solución con la plataforma de monitorización de la Consejería y su puesta en producción junto a su documentación relacionada. Tal como se ha mencionado anteriormente, este es un proyecto llave en mano y el proceso de implantación debe ser totalmente transparente para el usuario final, que, tras la migración, deberá poder acceder a sus datos/aplicaciones de la misma forma en la que lo hace con los sistemas actuales.

Una vez finalizada esta fase, el adjudicatario deberá presentar un documento acreditativo de buena implantación de la infraestructura siguiendo las buenas prácticas recomendadas por el fabricante de la solución. Dicho documento deberá estar emitido, sellado y firmado por parte del fabricante para cada una de los elementos de la infraestructura.

Con posterioridad a la migración de la infraestructura, el adjudicatario deberá retirar todos los equipos indicados por el Director de proyecto y todo el cableado sobrante.

En paralelo con las fases anteriores se impartirá el plan de formación reglada descrito más adelante, teniendo en cuenta que en las fechas en las que se imparta formación, no se realizarán tareas relacionadas con la instalación y configuración de la solución.

Igualmente, durante todas las fases, se tendrá en cuenta que para cada una de las intervenciones que formen parte de la programación de los trabajos será necesario presentar un informe, que deberá ser aprobado por el Director de Proyecto, y que, como mínimo, contendrá la siguiente información:

- Detalle de los trabajos de la intervención.
- Horario propuesto y duración estimada tanto de los trabajos y como de posibles cortes de servicio si los hubiera.
- Plan de restauración al punto inicial de partida de los trabajos a realizar.
- Recursos afectados.
- Personal involucrado en la realización de los trabajos.

Dicho informe relativo a cualquier trabajo/tarea a realizar, deberá ser entregado con una antelación mínima de 48 horas con respecto a la fecha propuesta del trabajo/tarea referenciada. En caso de no cumplirse este margen o que no se apruebe la documentación por parte de la Consejería, no podrán realizarse dichos trabajos/tareas.

Quedará reflejada en la oferta una planificación de la puesta en marcha que incluya una estimación del número de horas destinadas a cada una de las tareas indicadas anteriormente, así como las dependencias que existan entre ellas. No obstante, se recuerda que es un “llave en mano”a riesgo y ventura del adjudicatario.

- **FASE 3: SERVICIOS DE VALOR AÑADIDO Y SOPORTE AVANZADO.** Esta fase se iniciará después de la FASE 2 y finalizará a la conclusión del contrato (60 meses desde la firma del mismo). En esta fase se realizarán las sesiones de traspaso de conocimientos final, se realizará la consultoría sobre nuevas tecnologías de seguridad de la información y se realizarán las tareas de soporte y mantenimiento correctivo de toda la infraestructura ofertada.

  Se identifican los siguientes hitos en el proyecto:

- **HITO 1:** Suministro de todo el material, tanto hardware como software y licencias necesarios para la implantación de la infraestructura ofertada.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 50 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- **HITO 2:** Puesta en producción de toda la infraestructura. Esto incluye la instalación y configuración completa de todos los elementos, la migración a la nueva infraestructura y la realización de la formación y la entrega de documentación por parte del adjudicatario y la validación por parte de la Consejería. Este hito deberá ser alcanzado en los 8 meses posteriores a la firma del contrato. A partir de este hito empezará a computar el número de meses de soporte de la infraestructura que haya ofertado el adjudicatario, que incluirá el resto de la duración del contrato más el plazo de garantía. En caso de retraso en el cumplimiento de este HITO deberá efectuarse una ampliación del plazo de garantía, debido a la falta de ejecución de los trabajos requeridos.

  Desde el cumplimiento del HITO 2 y hasta el HITO 3 el adjudicatario prestará los servicios de soporte avanzado y valor añadido definidos en la FASE 3.

- **HITO 3:** Finalización del contrato. 5 AÑOS a partir de la firma del mismo.

NOTA: Todas las tareas de instalación y configuración tanto a nivel físico como lógico serán realizadas in-situ en las instalaciones de la Junta de Andalucía, y en cualquier caso contará con la presencia permanente de personal técnico de la Consejería, al que se dará traslado de las actuaciones realizadas, su justificación, el procedimiento seguido y las tareas de mantenimiento a realizar posteriormente.

La arquitectura integrada de todos los sistemas deberán cumplir su correspondiente diseño seguro, basado al menos en la mejora de la seguridad de las arquitecturas técnicas desde el diseño, mediante la definición de las políticas y controles de seguridad en cada escenario, considerando las buenas prácticas y referencias de arquitecturas seguras, como son las de las del CCN (Centro Criptológico Nacional de España) teniendo en cuenta la arquitectura técnica implantada. Básicamente deberán trabajar en la realización de:

- Procedimientos e instrucciones técnicas de bastionado seguro de componentes de arquitecturas técnicas.
- Recomendaciones de soluciones y tecnologías adicionales que puedan complementar la seguridad del servicio, sistema y/o infraestructura tecnológica.
- Guías de mejora de la seguridad de los procedimientos operativos de tecnologías de información.
- Revisiones de estado de seguridad y propuesta de mejora.
- La definición, creación de scripts y herramientas que sean capaces de detectar y comprobar si los controles de seguridad están aplicados.

5.4.7 Retirada y tratamiento medioambiental y seguro de los equipos

Al finalizar la ejecución de este proyecto, el Director del Proyecto podrá decidir que ciertos equipos de la infraestructura actual ya no tienen utilidad y los considera obsoletos. En tal caso, la empresa adjudicataria procederá a la retirada, borrado seguro y al tratamiento medioambiental de estos servidores con los seguros correspondientes y deberá presentar el documento acreditativo o certificado correspondiente.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 51 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

6 CONDICIONES GENERALES

6.1 Funciones y responsabilidades

La Consejería de Hacienda, Industria y Energía nombrará, entre su personal técnico cualificado, un Director del Proyecto, que la representará ante la Empresa Adjudicataria y dirigirá los trabajos asociados al Contrato de este pliego. En su caso, el Director del Proyecto podrá delegar ciertos aspectos de la gestión del contrato en el personal técnico de la Consejería que considere oportuno.

Los esfuerzos del Director del Proyecto deberán ir encaminados a:

- Asegurar el cumplimiento de lo establecido en los Pliegos de Cláusulas, tanto Administrativas como Técnicas.
- Asegurar el cumplimiento de los objetivos generales que la Consejería persigue con este contrato.
- Asegurar el cumplimiento de las mejoras aportadas por la oferta adjudicataria.
- Obtener la máxima calidad posible en los trabajos efectuados.

Por su parte la empresa adjudicataria nombrará un JEFE DE PROYECTO que la representará ante la Consejería de Hacienda, Industria y Energía y que dirigirá los trabajos asociados al contrato siguiendo las directrices que emanen de la Dirección del Proyecto. El Jefe de Proyecto tendrá a su cargo el equipo de proyecto necesario para la ejecución de las tareas asociadas al contrato. En la oferta deberá justificarse la idoneidad técnica del personal participante.

El licitador que presente la mejor oferta, deberá aportar el currículum vitae de las personas asignadas a la ejecución del contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional).

6.2 Lugar de entrega de los suministros y transporte

En caso de requerirse el suministro de elementos físicos durante la ejecución del contrato o en el periodo posterior de garantía, serán por cuenta del adjudicatario todos los gastos de transporte a los locales de la instalación, así como los gastos de seguro y otros en que se incurriera para el mismo.

La entrega de suministros se realizará en los CPDs de la Junta de Andalucía ubicado en las siguientes direcciones (salvo traslado de los dispositivos objeto del soporte a una ubicación distinta):

- CICA
  C/ Tarfia S/N, Edificio CICA
  Campus Universitario Reina Mercedes
  Edificio CICA
  Sevilla
- ZOCO
  Avda. de la Arboleda, S/N, Edificio ZOCO
  Tomares
  Sevilla
- Torretriana
  C/Juan Antonio de Vizarron S/N, Edificio Torretriana
  Sevilla

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 52 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

6.3 Inventariado de los bienes suministrados

En caso de suministrar bienes inventariables como por ejemplo servidores, se requiere que sean 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 23 de octubre de 2012, por la que se desarrollan determinados aspectos de la política informática de la Junta de Andalucía.

El etiquetado físico se realizará mediante etiquetas que proporcionará la Junta de Andalucía. El proceso completo de etiquetado debe realizarlo la empresa adjudicataria, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación. La empresa adjudicataria deberá realizar todos los pasos indicados en el procedimiento de inventariado de los bienes incluidos en la presente contratación 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 etiqueta adherida al equipo en los términos que describe el procedimiento de inventariado. Se proporcionará el procedimiento de inventariado al adjudicatario durante la ejecución del contrato.

Para aquellos bienes que permitan un etiquetado lógico, será obligatorio seguir una nomenclatura unificada para la Junta de Andalucía. Será responsabilidad del Organismo cumplir con la normativa de nomenclatura según se indique en el procedimiento de inventariado de bienes.

6.4 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.

6.5 Documentación entregable del proyecto

Para facilitar a la Dirección del Proyecto tanto las recepciones parciales como la recepción final del proyecto, deberán entregarse al menos los documentos indicados a continuación. La entrega de documentos debe realizarse a lo largo de la ejecución del proyecto, siendo necesaria la validación de los mismos por parte de la Dirección del Proyecto para darlos por definitivos. Una vez aprobados, el adjudicatario los almacenará y antes de finalizar el proyecto deberá realizar la entrega de todos los documentos aprobados junto con un inventario de los mismos.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 53 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Toda la documentación que vaya siendo entregada en formato digital se almacenará mediante alguna plataforma de almacenamiento online que indicará el Director del proyecto.

- Documentación de la FASE 0:
  - Propuesta del plan de facturación del contrato
  - Documento de diseño de implantación.
  - Plan de migración e integración.
  - Plan de pruebas.
  - Certificado emitido por el fabricante de la solución, para cada uno de los elementos ofertados, verificando que el diseño ha sido realizado correctamente y siguiendo las mejores prácticas recomendadas.
- Documentación de la FASE 1:
  - Albaranes de entrega de todos los elementos suministrados, en los que debe constar la fecha de entrega.
  - La documentación técnica del fabricante de todos los elementos hardware y software suministrados. Esta documentación es la única que podrá estar en idioma inglés de toda la documentación entregada.
  - Documento de ejecución del plan de pruebas.
  - Actualización del documento de diseño de implantación.
  - Actualización del plan de migración e integración.
  - Actualización del plan de pruebas.
  - Listado de elementos dados de alta en el inventario CRIJA incluyendo el siguiente detalle: número de inventario, marca, modelo, fabricante, número de serie, fechas de inicio y de finalización de garantía.
  - Documento de final de instalación y configuración de la infraestructura.
- Documentación de la FASE 2:
  - Actualización del documento de diseño de implantación.
  - Actualización de documentos de instalación.
  - Actualización del plan de migración e integración.
  - Actualización del plan de pruebas.
  - Actualización del documento de final de instalación y configuración de la infraestructura.
  - Plan de contingencia en caso de fallo de cualquier elemento de la infraestructura.
  - Documento con justificación de la no inclusión de configuraciones indicadas en las guias del CCN-CERT de cada fabricante.
- Documentación de la FASE 3:
  - Documento de titularidad de todos los elementos hardware, software y licencias que certifique que todos los items son propiedad de la Junta de Andalucía, y que indique el tipo de soporte contratado y la duración para todos los elementos ofertados.
  - Certificado emitido por el fabricante de la solución, para cada uno de los elementos ofertados, verificando que la instalación ha sido realizada correctamente y siguiendo las mejores prácticas recomendadas.
  - Documento acreditativo o certificado correspondiente de la retirada y tratamiento medioambiental y seguro de los equipos retirados.
  - En el ámbito de la consultoría sobre nuevas tecnologías de la seguridad de la información:
    - Presentación de la formación inicial sobre nuevas tecnologías de la seguridad de la información

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 54 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- Documentación de propuesta de rediseño de la infraestructura actual mediante el uso de nuevas tecnologías de la seguridad de la información.

- Otra documentación requerida:
  - Hoja de cálculo de seguimiento de entregables, que recogerá todos los entregables del proyecto y el estado de los mismos (entregado, validado, etc.). El adjudicatario deberá elaborar esta hoja de cálculo al inicio del proyecto y entregarla actualizada cada vez que cambie el estado de algún entregable, para facilitar el seguimiento de este ámbito del proyecto.
  - Informe final de ejecución del proyecto, que será requisito para la certificación del mismo. Dicho informe deberá planificarse por el adjudicatario desde el inicio del contrato, para que no quede nada sin ejecutar. Contendrá al menos:
    - Relación pormenorizada de los trabajos realizados, incluyendo tareas de puesta en marcha, consultoría, formación, bolsas de horas, etc.
    - Relación pormenorizada de los suministros realizados.
    - Relación pormenorizada de la documentación entregable proporcionada.
  - Listado de elementos en garantía con indicación al menos de:
    - Las coberturas de los servicios de soporte/mantenimiento de acuerdo a los requisitos del Pliego y a los compromisos adquiridos por el adjudicatario en su oferta.
    - Los números de teléfono y/o direcciones Web habilitados para reportar incidencias, usuarios de soporte asignados y los horarios de atención.
    - Las fechas de inicio y finalización del servicio.
  - Manuales/Presentaciones de todos los cursos de formación reglada/a medida/transferencias de conocimiento (deberán enviarse de manera previa al inicio de las sesiones de formación).
  - Actas de todas las reuniones de seguimiento del proyecto.
  - Cualquier otra documentación generada durante el proyecto.

6.6 Formato de entregables

Toda la documentación del proyecto tendrá que ser entregada en castellano (los manuales originales de los fabricantes es la única documentación que será admitida en ingles), tanto en papel (encarpetada o encuadernada) como en los siguientes formatos electrónicos:

- Formato editable ISO/IEC 26300 (formato OpenDocument de OASIS).
- Formato no editable para su preservación a largo plazo ISO 19005-1:2005 (PDF/A-1).

La Consejería facilitará al adjudicatario plantillas OpenDocument con el formato de documentación que deberá utilizarse en la ejecución (estilos, logotipos, etc).

6.7 Confidencialidad

El adjudicatario deberá garantizar la confidencialidad e integridad de los datos manejados y de la documentación facilitada.

En este sentido, deberá sujetarse a los preceptos legales en materia de protección de datos personales recogidos en la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril "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

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 55 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

deroga la Directiva 95/46/CE (Reglamento general de protección de datos)" y en el Esquema Nacional de Seguridad (ENS).

Si alguna de las personas integrantes de la empresa adjudicataria destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las instrucciones de la Consejería, la empresa contratada será responsable de las infracciones cometidas.

Además, deberán cumplir con las medidas de seguridad, normas y procedimientos que en cada caso establezca esta Consejería.

6.8 Conformidad con el Esquema Nacional de Seguridad

Según lo dispuesto por la Disposición adicional primera de la LO 3/2018 de Protección de Datos Personales y Garantía de los derechos Digitales, el Esquema Nacional de Seguridad incluirá las medidas que deberán implementarse a los tratamientos de datos personales realizados en el ámbito del sector público. Por tanto, se aplicarán las medidas de seguridad establecidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015, de 23 de octubre. Adicionalmente se aplicarán las medidas de seguridad que se definan por la Dirección del Proyecto durante la ejecución del mismo.

Por lo anterior, se exige en el pliego el requerimiento de Certificación de Conformidad con el ENS a la empresa adjudicataria, por lo que se requiere que el adjudicatario disponga de la **Certificación de Conformidad con el Esquema Nacional de Seguridad para sistemas de información de categoría ALTA**, dada la identificación a fecha actual de determinados sistemas de información de categoría ALTA en el ENS.

Caso de que el adjudicatario no disponga de la Certificación de Conformidad para sistemas de información de categoría ALTA, se le otorgaría un plazo máximo de 6 meses para la obtención de la misma, contados a partir de la fecha de adjudicación/formalización del contrato.

6.9 Propiedad intelectual

Toda la documentación generada durante la ejecución de este contrato es propiedad exclusiva de la Junta de Andalucía, sin que el contratista pueda conservarla, ni obtener una copia de la misma o facilitarla a terceros sin la expresa autorización de esta Consejería, que la daría en su caso previa petición formal y escrita del contratista con expresión del fin al que se destinara y únicamente para la consecución de dicho fin.

6.10 Esquema Nacional de Seguridad

En cumplimiento con lo dispuesto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y en el Real Decreto 951/2015, de 23 de octubre, por el que se modifica el anterior, el adjudicatario incluirá referencia precisa, documentada y acreditativa de los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, sin menoscabo de lo indicado en el Reglamento (UE)

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 56 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

2016/679 del Parlamento Europeo y del Consejo de 27 de abril "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 (Reglamento general de protección de datos)".

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

En caso de cambios en la normativa referente al Esquema Nacional de Seguridad el adjudicatario deberá entregar nuevas referencias precisas, documentadas y acreditativas de los sistemas.

EL JEFE DE SERVICIO DE SISTEMAS HORIZONTALES

Francisco José Doménech Colomer

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 57 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

7 ANEXO. CLÁUSULAS GENÉRICAS DE PRODUCCIÓN APLICABLES

El objeto de este anexo es informar a los adjudicatarios de determinadas cláusulas genéricas en aspectos de producción y operación de sistemas limitado al ámbito de la solución del presente pliego, y que podrá suponer que se pueda solicitar al adjudicatario la realización de posibles tareas para el cumplimiento de estas cláusulas. Para la Consejería, podrá suponer tareas de coordinación y seguimiento de la ejecución de las tareas necesarias.

7.1 Información para la Puesta en Explotación de la Infraestructura

Respecto a la información a proporcionar por el adjudicatario para la puesta en explotación del equipamiento, a modo de ejemplo, pero con carácter no exclusivo, se debe tener en cuenta los siguientes aspectos:

- **Manual de instalación del sistema**
  - La empresa adjudicataria deberá incluir en los procedimientos de instalación segura, aquellos aspectos exigidos por el ENS (retirar cuentas y contraseñas estándar, "mínima funcionalidad" y "seguridad por defecto"), con objeto de mantener solo las funcionalidades mínimas deshabilitando o eliminando todas aquellas que no sean necesarias, y aplicando la regla de "seguridad por defecto". Para ello, se pueden seguir las guías de instalación segura elaboradas por el Centro Criptológico Nacional (Guías CCNSTIC)
- **Manual de operación** del sistema (procedimientos de inicio y parada del sistema, tareas periódicas de mantenimiento, etc.)

7.2 Aceptación de los trabajos

Para efectuar la aceptación final de los trabajos del proyecto, la Consejería efectuará las pruebas que estime oportunas de verificación y validación del objeto del presente documento.

En estas revisiones, se podrán realizar pruebas de calidad (funcionamiento, configuración, tuning) y pruebas de rendimiento, diseñadas y realizadas de forma específica para la solución, y en la que se podrá solicitar a la empresa adjudicataria el soporte necesario para el diseño de estas pruebas.

Para sistemas de categoría igual o superior a MEDIA, además la Consejería podrá asegurar la puesta en explotación de la infraestructura con la realización de análisis de vulnerabilidades y pruebas de penetración de manera previa, como requisito de la entrada en servicio de la aplicación

7.3 Supervisión de los Sistemas

Se exigirá al adjudicatario el objetivo de asegurar que el sistema se implanta, mantiene y se presta soporte sobre el mismo de acuerdo con las necesidades manifestadas por el Director del Proyecto y con las especificaciones incluidas en los pliegos de prescripciones técnicas y cláusulas administrativas de acuerdo con las indicaciones del Director del Proyecto.

Debe proporcionarse al Director del Proyecto, acceso a la información necesaria sobre el funcionamiento del sistema que les permita ejercer sus funciones de coordinación, supervisión y control. Igualmente, debe proporcionarse, la información necesaria para asegurar que el sistema funciona conforme a sus especificaciones.

El sistema debe guardar registro de auditoría de todas las acciones que se realicen sobre el mismo.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 58 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

7.4 Trazabilidad y auditoría

El sistema debe proporcionar confianza y transparencia sobre la confidencialidad y correcta tramitación de los procesos de los que se compone y, en caso de discrepancias respecto a su resultado, facilitar la puesta a disposición de la información necesaria para la resolución eficaz de los procedimientos de reclamación.

Deben disponer de toda la información de trazabilidad y auditoría necesaria para la toma de decisiones respecto a las comunicaciones que reciban.

El sistema debe guardar registro de todas las acciones sobre el mismo necesarias para una correcta auditoría de los procesos que se implementan en la aplicación, que permita resolver cualquier reclamación que se produzca, incluyendo el registro de actividad de la aplicación que determine el Director del Proyecto, a modo de ejemplo el inicio y cierres de sesión correctos y fallidos, funciones y transacciones ejecutadas por los usuarios, etc.

7.5 Software base a utilizar. Software comercial. Licencias

Las versiones del software a emplear serán versiones lo suficiente estables para garantizar que no compromete aspectos de seguridad, pero a la vez lo suficientemente actualizadas para disponer del soporte estándar ofrecido por el fabricante durante el mayor tiempo posible, sin necesidad de migración del producto.

El software entregado por la empresa adjudicataria deberá funcionar con componentes de software base actualizados, durante todo el periodo de tiempo de vigencia del contrato, por lo que puede suponer la necesidad por parte de la empresa adjudicataria de adecuación del software a las nuevas versiones de los componentes de software base, con motivo de la posible obsolescencia tecnológica en las que se despliegue el software entregado.

Por lo tanto, el sistema deberá adaptarse a los cambios de tecnologías y versiones de software base que se realicen sobre la plataforma.

Para facilitar este proceso, la Consejería ofrecerá de forma periódica información detallada de las recomendaciones de los componentes y versiones recomendadas de los productos de software base a utilizar, incluyendo componentes de servidores de aplicaciones, Base de Datos y plataforma web.

La empresa adjudicataria deberá dar información del entorno tecnológico en el que realizará los trabajos o que requiere para su realización, incluyendo a modo de ejemplo estos componentes:

- Versiones de sistemas operativos.
- Bases de datos.
- Servidores de aplicaciones.
- Sistemas de Gestión Documental.
- Sistemas de BI.
- Otros sistemas

Si para la implantación de la solución ofertada se requiriese un determinado software o herramienta que requiera algún tipo de licencia comercial, estas licencias deberán ser proporcionadas por la empresa adjudicataria durante todo el periodo de tiempo de vigencia del contrato.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 59 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Asimismo se deberá justificar en la oferta la necesidad de dicho software, las ventajas que aporta al proyecto e incluir un análisis completo y detallado de los costes, incluyendo modelo de licenciamiento, costes de licenciamiento y costes de mantenimiento de las licencias (teniendo en cuenta el número de usuarios previstos) e incluso posibles costes de soporte que pudieran ser necesarios aún en el caso de tratarse de software libre.

Para los componentes de software base, por ejemplo servidores de aplicaciones, se deberá dar preferencia al uso de software libre y, caso necesario, la empresa adjudicataria deberá dar información y proporcionar las posibles licencias que sean necesarias para el despliegue de la solución.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 60 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

8 ANEXO. CLÁUSULAS GENÉRICAS DE SEGURIDAD APLICABLES

8.1 Políticas y procedimientos de seguridad

El personal de la empresa adjudicataria realizará los trabajos bajo las medidas de seguridad, normas y procedimientos que determine la Dirección del Proyecto.

8.2 Cumplimiento medidas ENS

La empresa adjudicataria deberá garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación. Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando que el sistema de información recae en la categoría de seguridad ALTA conforme a los criterios establecidos en el anexo I del ENS.

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.ccn-cert.cni.es/), así como a las recomendaciones de AndalucíaCERT, como centro especializado en la materia en el ámbito andaluz.

Caso de que la empresa adjudicataria utilice algún componente relacionado con aspectos de la seguridad de la información, deberá incluir referencia precisa, documentada y acreditativa de los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados recogida en el apartado 4.1.5 en el Anexo II del ENS, que requiere que las funcionalidades de seguridad y su nivel de estos componentes, hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

8.3 Aspectos de seguridad a tener en cuenta para la Plataforma de Producción

8.3.1 Accesos remotos

Para el caso de acceso remotos, el acceso de los técnicos del equipo de proyecto de la empresa adjudicataria será autorizado por el Director de Proyecto de la Consejería. El modo de acceso será tal que garantice la seguridad de operación y explotación del sistema así como el objetivo de almacenar y gestionar las solicitudes de servicio e incidencias que se produzca durante la ejecución del contrato. Para ello se proveerá acceso a través de VPN a las personas designadas por el adjudicatario a tales efectos. Todos los costes asociados a la línea de comunicación y la conexión a la red corporativa de la Junta de Andalucía correrán por cuenta del adjudicatario.

La empresa adjudicataria deberá cumplir con la política de acceso remoto que pudiera existir en la Consejería durante todo el periodo de vigencia del contrato, que pudiera incluir, entre otros aspectos: mecanismo de identificación y autenticación robusto, red privada virtual a utilizar, funciones

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 61 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

permitidas y datos accesibles desde acceso remoto, tiempo máximo para cerrar sesiones inactivas, activación de los registros de actividad, etc.

8.3.2 Explotación y monitorización de sistemas

El sistema ofrecerá seguridad frente a virus informáticos y otro tipo de programas o códigos nocivos, sin que esto impida el funcionamiento normal de la aplicación.

Se preverá cómo deben realizarse las salvaguardas del sistema en la infraestructura de salvaguarda de la Consejería.

El sistema funcionará en alta disponibilidad y preverá los mecanismos para minimizar el tiempo que el servicio esté interrumpido y los efectos que ello tenga sobre los usuarios finales, debiendo ofrecer la empresa adjudicataria los mecanismos necesarios para conseguir la alta disponibilidad de todos los componentes que forman parte de la solución.

Se documentarán y proporcionarán los medios para obtener e integrar en los sistemas de monitorización de la Consejería los indicadores y parámetros necesarios para asegurar la disponibilidad del sistema y sus componentes con el nivel de rendimiento mínimo definido.

8.3.3 Gestión de usuarios

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales, concretamente:

- Los usuarios solo deberán tener acceso a aquellos recursos que necesiten para el desempeño de sus funciones, como una medida de carácter básico.
- El sistema debe garantizar de forma inequívoca y personalizada la identificación de todo usuario que intente acceder, y la verificación de su autorización .
- Si la autenticación está basada en contraseñas, se deberá garantizar que el almacenamiento de las mismas en el sistema garantice su confidencialidad e integridad.

En virtud de lo establecido en el artículo 14.4 del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad, para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso y de qué tipo son éstos. El certificado electrónico podrá utilizarse como medio de autenticación de usuarios, si bien no de modo exclusivo, debiéndose disponer de un medio de autenticación alternativo a su utilización.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar (roles, gestión de login y password,....) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta de Andalucía haya provisto. Dichas Directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

8.3.4 Protocolos de comunicaciones inseguros

La empresa adjudicataria no podrá utilizar aplicaciones HTTPS con suites débiles que podrían comprometer la seguridad de los servicios y de la información.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 62 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

9 ANEXO: INSTALACIONES ELÉCTRICAS Y CABLEADO DE COBRE Y FIBRA

9.1 INSTALACIÓN ELÉCTRICA RACKS

El adjudicatario se encargará de suministrar e instalar cuatro líneas eléctricas a cada rack. Cada una de las 4 líneas eléctricas constará de: Interruptor automático 2x32A curva "D", protección diferencial 2x40A con sensibilidad de 300mA súper inmunizado, manguera libre de halógenos de aproximadamente 3 metros acabada en toma cetac de 32A, pequeño material necesario para la instalación como pueden ser prensaestopas o terminales. El adjudicatario instalará las protecciones eléctricas en cajas de blindobarras que aportará la propiedad.

9.2 CABLEADO DE COMUNICACIONES

La instalación de cableado que se ejecute cumplirá los requisitos establecidos en la Orden de 2 de junio de 2017, reguladora de los requisitos necesarios para el diseño e implementación de infraestructuras de cableado estructurado y de red de área local inalámbrica en el ámbito de la Administración de la Junta de Andalucía, sus Entidades Instrumentales y los Consorcios del Sector Público Andaluz; con corrección de errores publicado en el BOJA número 142 de 26 de julio de 2017.

9.2.1 Enlaces

Se realizará el tendido siguiendo las directrices indicadas a continuación:

- Evitar torceduras y tirones, así como radios de curvatura inferiores a 5 cm.
- No sobrecargar las canalizaciones y bandejas.
- Evitar el estrangulamiento de los cables con las bridas de fijación.
- No agrupar los cables del tendido horizontal en mazos de más de 40 unidades.
- La empresa adjudicataria proveerá las canalizaciones y rejillas necesarias para el tendido completo del cableado, en caso de ser necesario.
- Para el tendido de la fibra óptica horizontal, se hará uso preferentemente de canalizaciones ancladas en el techo del CPD, con la excepción del cableado que fuera necesario ubicar por suelo debido a las características de las cabinas o mainframes.
- Para el tendido del cableado de cobre horizontal, se hará uso de canalizaciones bajo el suelo técnico que partirán por un lado de los armarios de comunicaciones y con destino a determinados racks, así como de diversos paneles en suelo frente a las maquinas que lo requieran y que podrán ir tanto a los armarios de comunicaciones como a los racks que lo requieran. El CPD está dotado de canalizaciones bajo el suelo técnico. En caso de tener que ampliar tramos o instalar nuevos será por cuenta del adjudicatario.

Los cables de cobre S-FTP se instalarán por las canalizaciones rejiband actuales instaladas bajo el falso suelo del CPD, en caso de necesitar ser ampliada la canalización correrá por cuenta del adjudicatario. Las terminaciones de los cables de cobre FTP en todos los racks se realizará en el interior de los mismos en la posición que designe la propiedad, en función de la disponibilidad de espacio actual.

Se requiere que el cableado estructurado de cobre horizontal del CPD sea FTP Categoría 7 con conectores RJ-45 cat. 6A, para permitir velocidades de transmisión de hasta 10 Gbps.

Las características de los cables de cobre a instalar serán las siguientes:

- Cableado S/FTP categoría 7/Clase FA según ISO/IEC 11801 2ª edición incluidas enmiendas 1 y 2 o equivalentes.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 63 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

- El cableado debe estar doblemente apantallado.
- Debe cumplir o superar las especificaciones de la norma EN 50173- 1 2ª edición y de la ISO/IEC 11801 2ª edición para requerimientos de canal para soportar 10GBASE-T (debe ser instalado como parte de una solución completa de cableado estructurado que soporte velocidades de transmisión desde 10Gbps en longitudes de 100 metros para pruebas de canal).
- El sistema debe garantizar el correcto funcionamiento de alimentación por el par trenzado POE y POE Plus.
- Los cables tendrán cubiertas libres de halógenos de baja emisión de humos (LSZH).
- El cable debe cumplir mínimo con los siguientes rangos de temperatura para operaciones: entre - 20°C y +60°C.

Las características de los paneles repartidores a instalar serán las siguientes:

- Los paneles de parcheo del cableado de cobre serán Categoría 6A, con 24 conectores hembra RJ-45, aptos para soportar cables FTP, intercambiables fácilmente en el futuro con conectores Categoría 7.
- Deben ser de 24 conectores y 1U de altura.
- Deben poseer salidas RJ45 con conectores que igualen o excedan las especificaciones de STP
- categoría 6A/Clase EA.
- Debe tener 19 pulgadas de ancho para ser instalados en los racks que se suministrarán.
- Los conectores de los paneles deben permitir enlaces desde 3m a 90m, y hasta 4 conexiones en el mismo canal.
- Los paneles serán angulados para disponer de solución de alta densidad evitando los pasahilos horizontales y facilitando gestión del sistema.
- Se dispondrá de organizadores laterales por cada panel para la correcta organización de los latiguillos.
- Como mínimo, por cada 6 pares de 24 puertos, se dispondrá un pasahilos horizontal de 2U con tapa.

Las características de los conectores serán las siguientes

- Deben poseer salidas RJ45 que igualen o superen las especificaciones de FTP categoría A/Clase EA.
- Los conectores deben permitir enlaces desde 3m a 90m, y hasta 4 conexiones en el mismo canal.
- Deben terminarse mediante herramienta de engaste específica, para control de la inserción de todos los pares simultáneamente.
- Debe estar certificado para cumplir o superar las especificaciones de alimentación a través del par trenzado, POE y POE Plus.
- El conector servirá para terminar conductores sólidos de 22 a 26 AWG.
- Los conectores deberán ser compatibles con el cableado utilizado, con objeto de garantizar la completa interoperabilidad mecánica de los componentes.

Los cables de fibra óptica se instalarán por las canalizaciones actuales instaladas en el CPD colgadas del techo por encima de los racks, desde las que se accede a la parte superior de los mismos. En caso de tener que ampliar las canalizaciones será por cuenta del adjudicatario.

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 64 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

Las terminaciones de los cables de fibra óptica en todos los racks se realizarán en la zona superior de los mismos en las U's mas altas posible según indique la propiedad, en función de la disponibilidad de espacio actual.

Las longitudes son variables pudiendo obtenerse en la visita concertada.

Para la fibra óptica se usarán cables de 24 fibras ópticas multimodo 50/125 µm OM3 o superior preconectorizados tipo MPO terminado en ambos extremos con cassettes de 12 conectores LC duplex, para poderse utilizar con 10 Gb y en el futuro para 40 G, o 100 G, cambiando los cassettes de terminación. Se indicará expresamente en la oferta los cambios a realizar en la instalación para pasar de 10 Gb a 40 Gb y a 100 Gb.

Las características de los cables y casetes de fibra a instalar serán las siguientes:

- Fibra óptica multimodo de 50/125 OM3 conforme a la normativa EN 50173-1 2ª edición, la ISO/IEC 11801 2ª edición o equivalentes.
- Los cables de fibra serán preconectorizados y se insertarán en bandejas de alta densidad anguladas escalables que usan módulos de 24 fibras, para realizar la transición desde el conector MPO a conectores LC.
- Los cables de fibra óptica estarán probados en fábrica. Los conectores de los extremos serán MPO/MTP de 24 fibras, según las normas IEC 61754-7 y TIA 604-5 o equivalentes.
- Todo el cableado de fibra óptica debe estar preparado para la migración a 40 y 100Gigabit.
- Se garantizará el balance de potencia requerido por las aplicaciones 40GBASE-SR4 y 100GBASESR10 con 2 cassettes en un mismo enlace.
- Los cables tendrán cubiertas libres de halógenos de baja emisión de humos (LSZH) y cubierta protectora frente a aplastamiento y cargas de tendido en bandejas rejiband, válida para interior y exterior.
- Debe soportar mínimo las siguientes aplicaciones: IEEE 802.3 (1000BASE SX/LX, 10GBASE-SR, 10GBASE-SW, 10GBASELX4), ATM (155 Mb/s, 622 Mb/s, 1.2 y 2.4 Gb/s) y estará preparado para las aplicaciones 40GBASE-SR y 100GBASE-SR.
- El rango mínimo de temperatura que la fibra óptica debe soportar sin que su operación y rendimiento se afecten debe estar entre -20° C y +50° C.
- La Longitud de onda de la fibra debe cumplir 850/1300 nm.
- El Ancho de Banda de la fibra deberá mínimo cumplir los 1.500 MHz a 850 nm y 500 MHz a 1300 nm.
- La fibra óptica deberá soportar velocidades de 10 Gbps para longitudes de 550 mts a 850/1300 nm y 40/100 Gbps para longitudes de 150 mts.
- La atenuación máxima permitida del cable será de 3.5 dB/Km a 850 nm y 1.5 dB/Km a 1300 nm.
- La pérdida de inserción máxima del cable tipo MPO será de 0,30 db
- La pérdida mínima de retorno del cable tipo MPO será de 25 db
- Las bandejas de terminación de tamaño 1U tendrán capacidad para hasta 4 cassettes de 24 fibras.
- La solución MPO/MTP propuesta debe garantizar hasta 6 cassettes en un mismo enlace 10GBASE-SR.
- Se dispondrá de 2 organizadores laterales por cada bandeja, para la correcta organización de los latiguillos.
- Como mínimo, por cada 6 paneles de 24 puertos, se dispondrá un pasahilos horizontal de 2U.
- La pérdida de inserción máxima del cassette de conexión sera de 0,4 db
- La pérdida mínima de retorno del cassette de conexión será de 25 db

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 65 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	

9.2.2 Provisión de latiguillos de cobre y fibra

Las características de los latiguillos de cobre serán las siguientes:

- Debe cumplir o superar las especificaciones de la EN 50173 1 2ª edición y de la ISO/IEC 11801 2ª edición o equivalentes, para requerimientos de canal para soportar Categoría 6A/Clase EA.
- Los latiguillos para la conexión de los equipos del usuario final deben estar construidos con conectores macho (plugs) tipo RJ45 en ambos extremos. El cable utilizado para estos latiguillos deberá ser cable de cobre categoría 7 y tener las mismas características de desempeño nominales del cableado horizontal especificado.
- Los latiguillos tendrán la longitud apropiada para minimizar el impacto de los cables sobrantes en los armarios racks.
- Los latiguillos de parcheo deben tener una construcción flexible y apantallada, garantizando la continuidad de la malla en todo el canal de cableado.
- Los latiguillos tendrán cubiertas libres de halógenos de baja emisión de humos (LSZH).
- Los latiguillos deberán ser originales de fábrica y precertificados por el fabricante como estipula EN 50173 1 2ª edición y de la ISO/IEC 11801 2ª edición o equivalentes, deberán venir en su bolsa original de embalaje tal como salen de la fábrica. No se aceptarán latiguillos fabricados de forma artesanal, ya que no se podría garantizar el cumplimiento de las normas citadas anteriormente.

Las características de los latiguillos de fibra serán las siguientes:

- Se utilizarán latiguillos de fibra óptica dúplex con conectores de ferrule cerámico LC dúplex multimodo OM3, según normativa internacional ISO/IEC 11801 2nd Ammendment 1.1 y 2.
- Todos los latiguillos estarán testeados según los protocolos de test de la normativa ISO/IEC 11801 2nd Ammendment 1.1 y 2 y estarán provistos de un pulido de alta calidad.
- Los latiguillos tendrán cubiertas libres de halógenos de baja emisión de humos (LSZH).
- Los latiguillos deberán ser compatibles con el cableado utilizado, con objeto de garantizar la calidad del sistema.
- Los latiguillos tendrán la longitud apropiada para minimizar el impacto de los cables sobrantes en los armarios racks.
- La atenuación máxima del latiguillo será de 0,20 db.
- La pérdida mínima de retorno del latiguillo de conexión será de 30 db

FRANCISCO JOSE DOMENECH COLOMER		10/05/2020	PÁGINA 66 / 66
VERIFICACIÓN	NJyGwUaoMLJ3KEF2vr1a0pJBgu5oSt	https://ws050.juntadeandalucia.es/verificarFirma	