PLIEGO DE PRESCRIPCIONES TÉCNICAS

SUMINISTRO DE SOLUCIÓN ANTIVIRUS DE PUESTO DE TRABAJO Y SERVIDOR CON SUSCRIPCIÓN DE ACTUALIZACIONES Y SOPORTE PARA LA CONSEJERÍA DE ECONOMÍA, HACIENDA Y ADMINISTRACIÓN PÚBLICA

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 1 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

CONTENIDO

1 DEFINICIONES, ABREVIATURAS Y ACRÓNIMOS....3

2 INTRODUCCIÓN....4

3 ALCANCE....5

4 OBJETO DEL PLIEGO....5

5 PRESCRIPCIONES TÉCNICAS....5

5.1 Descripción del entorno afectado....5
5.2 Situación a alcanzar mediante la presente contratación....6
5.3 Requisitos técnicos....6
5.4 Dimensionamiento....9
5.5 Servicios requeridos....9
5.5.1 Auditoría de la implantación (sólo en caso de mantener la solución del fabricante actual)....9
5.5.2 Servicio de implantación y transferencia de conocimientos (sólo en caso de cambio de fabricante de la solución)....9
5.6 Mejoras....11
5.7 Condiciones a las que debe ajustarse la suscripción de actualizaciones y soporte durante el plazo de vigencia de la garantía....11

6 CONDICIONES GENERALES....12

6.1 Funciones y responsabilidades....12
6.2 Plan de proyecto....12
6.3 Acreditación como partner....12
6.4 Documentación entregable del proyecto....13
6.5 Formato de entregables....13
6.6 Garantía técnica....14
6.7 Confidencialidad....14
6.8 Propiedad intelectual....14
6.9 Esquema nacional de seguridad....15

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 2 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

1 DEFINICIONES, ABREVIATURAS Y ACRÓNIMOS

La Consejería: Consejería de Economía, Hacienda y Administración Pública.

El Servicio: Servicio de Producción de la Dirección General de Política Digital de la Consejería de Economía, Hacienda y Administración Pública..

Servicio de Producción: Servicio de Producción de la Dirección General de Política Digital de la Consejería de Economía, Hacienda y Administración Pública..

EndPoint: Punto final en donde se instala un agente de antivirus, ya sea servidor, puesto de trabajo, dispositivo móvil, etc.

CEHAP: Consejería de Economía, Hacienda y Administración Pública..

TIC: Tecnologías de Información y Comunicaciones.

ENS: Esquema Nacional de Seguridad.

DLP: Prevención de robo de información (Data Leak Prevention).

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 3 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	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 y mantenimiento de antivirus de puesto de trabajo de la Consejería de Economía, Hacienda y Administración Pública (CEHAP).

La situación actual de las redes de datos, compuestas por numerosos elementos de red que dan soporte a servicios de voz, datos y video, cada uno de estos tráficos con unos requerimientos diferentes, proporcionando accesos tanto a usuarios dentro de la red como a usuarios externos, conectadas a Internet y a redes de otros organismos y, por otra parte, la evolución de los virus, ataques y amenazas procedentes de Internet o de los propios usuarios de la red, hacen necesario elaborar una estrategia completa de seguridad en varios niveles o capas, aplicando las correspondientes medidas de seguridad en cada nivel, como establece el Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010 de 3 de enero.

La CEHAP da un servicio 24x7 los 365 días del año en alta disponibilidad (tal y como establecen la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público). Dicho servicio se presta tanto a la ciudadanía como a los propios profesionales de la Administración Pública, por este motivo, el no mantener la infraestructura de antivirus actualizada acorde a los niveles de servicio requeridos puede provocar problemas que interfieran en la calidad y disponibilidad de la información a la ciudadanía y al personal de esta Consejería y de la Junta de Andalucía.

Hay que tener en cuenta que un fallo o un ataque a un componente de la red puede producir una caída en todo el sistema, si no se ponen los medios necesarios para prevenirlos o paliar sus consecuencias. El impacto de un fallo en la red puede implicar diversos niveles de gravedad, desde tiempo de inactividad de la red, los sistemas y aplicaciones que soporta, hasta pérdidas económicas o deterioro del prestigio de la organización. El carácter crítico que los activos TIC tienen para los servicios de administración electrónica que se ofrecen a ciudadanos y empresas, así como para el desarrollo de la actividad diaria de los empleados públicos, conduce a la necesidad de mitigar de modo eficiente los incidentes de seguridad. La Dirección General de Política Digital, como responsable de la explotación y buen funcionamiento de estos activos, solicita a través de este expediente la adquisición del derecho de uso de una solución software para detección de código malicioso, buscándose una mayor fiabilidad, seguridad, calidad y soporte en la seguridad informática de forma que se pueda proporcionar una seguridad más eficaz ante nuevas amenazas para todos los puestos de trabajo y todos los servidores de la CEHAP.

La línea de defensa más interna de la red debe estar formada por un sistema de seguridad para protección de los propios equipos de los usuarios y los servidores, que constituiría una de las medidas de protección mínimas recogidas en el ENS. Concretamente se trata de una medida del marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 4 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

integral de componentes, en el área de explotación (medida op.exp.6 en el Anexo II, apartado 4.3.6), que se refiere a la protección frente a código dañino y que aplica a todos los sistemas instalados en la red corporativa. Considerando el ENS en el apartado 4.3.6 como código dañino a los virus, gusanos, troyanos, programas espía (spyware) y, en general, todo código conocido como malware y obligando en este apartado el Real Decreto a disponer de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante

En la actualidad, el crecimiento en cuanto a servicios que presta la CEHAP a la ciudadanía ha provocado un crecimiento del parque informático y la previsión es de un mayor crecimiento por lo que es necesario el suministro de nuevas licencias de la solución de antivirus y la suscripción de las actualizaciones y del soporte para las mismas para cubrir las necesidades actuales y futuras.

3 ALCANCE

El presente documento se refiere en general a la Infraestructura Tecnológica de la CEHAP y en particular a la solución de antivirus de puesto de trabajo y de servidores instalada en la Consejería de Economía, Hacienda y Administración Pública de la Junta de Andalucía.

4 OBJETO DEL PLIEGO

- Suministro de solución antivirus de puesto de trabajo y servidor con suscripción de actualizaciones y soporte. La suscripción de actualizaciones y el soporte estará vigente al menos hasta el 31 de enero de 2023 en garantía, siendo objeto de valoración su ampliación en el tiempo.

5 PRESCRIPCIONES TÉCNICAS

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

5.1 Descripción del entorno afectado

La Consejería dispone actualmente de 1482 licencias de Trendmicro Smart Protection Complete, como producto antivirus de puesto de usuarios y servidores con fecha de finalización de soporte y derecho de actualizaciones de 31 de enero de 2019.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 5 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

5.2 Situación a alcanzar mediante la presente contratación

Mediante esta contratación se pretende ampliar el número de licencias antivirus de puesto de trabajo y servidor sin incluir la funcionalidad de DLP (dicha funcionalidad está incluida en el licenciamiento actual pero no está en uso ni se requiere en esta nueva contratación), hasta alcanzar un mínimo de 2500 licencias, así como contar con el soporte y mantenimiento y con las actualizaciones de los patrones y firmas de virus para la totalidad de las licencias.

Todas las licencias deberán integrarse con la infraestructura actual de antivirus de la CEHAP, salvo que el licitador optara por sustituir la solución actual de antivirus por una distinta, en cuyo caso deberá realizar el despliegue completo de la solución ofertada según se describe en "5.5.2 Servicio de implantación y transferencia de conocimientos (sólo en caso de cambio de fabricante de la solución)".

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

Sistemas	**N.º mínimo de licencias**
Antivirus de puesto de trabajo y servidores sin funcionalidad de DLP, con suscripción de actualizaciones de versiones, patrones y firmas de virus y soporte	Ampliación de licencias para alcanzar el mínimo de 2500. La suscripción estará vigente durante el plazo de garantía y debe cubrir la totalidad de las licencias (las actuales y la ampliación ofertada).

Igualmente se requieren los siguientes servicios:

Servicios	**Observaciones**
Auditoría de la implantación actual	En caso de que se oferte la solución del fabricante actual
Servicios de implantación, configuración y traspaso de conocimientos	En caso de que se oferte cambio de fabricante.

5.3 Requisitos técnicos

- Integración con la infraestructura actual de antivirus de Endpoint[1] de CEHAP tanto en hardware como en software y gestión del equipamiento.
- Se debe garantizar la continuidad de los servicios en las mismas condiciones que en la actualidad.
- Se debe tener una arquitectura que garantice la robustez de la solución en términos de disponibilidad, tolerancia a fallos y seguridad.
- La solución debe ser gestionable de manera remota desde el puesto de trabajo local.
- Soporte de funciones de supervisión y gestión centralizada.
    - Visibilidad y administración centralizada

1Ver apartado de Definiciones al inicio del documento

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 6 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

  - Gestión de políticas y amenazas
- Protección de endpoint con los siguientes sistemas operativos:
  - MAC (OS X 10.8 o superior)
  - Windows (XP, 7, 8, 10, server 2003, server 2008, server 2012, server 2016)
  - Smartphones y tablets (IOS 5 o superior, ANDROID 3 o superior y Windows Phone 8 o superior)
  - Endpoints virtualizados (VDI)
- Posibilidad de analizar unidades USB y extraíbles.
- Posibilidad de analizar el correo electrónico.
- Posibilidad de analizar servidores de ficheros.
- Protección multi-capa: Proporcionando múltiples capas de protección en forma de motores tradicionales y de última generación:
  - Motores antimalware basados en firmas y reputación.
  - Motores de detección avanzada para detección de amenazas desconocidas: Detección de secuencias de comandos, inyecciones, ataques de tipo ransomware, ataques en memoria y ataques en el navegador. Evaluando el comportamiento de archivos ejecutables y de los procesos del sistema. Con mecanismos de backup y recuperación de ficheros ante un intento de cifrado no autorizado.
- Posibilidad de detectar y bloquear de amenazas contenidas en scripts.
- Prevención de exploits.
- Posibilidad de bloquear comunicaciones de tipo comando y control (Command and Control - C&C)
- Posibilidad de detección y eliminación del malware, spyware, adware y otras amenazas, que permita aplicar múltiples opciones según el tipo de amenaza parada (limpiar el fichero, ponerlo en cuarentena, eliminar un correo o solamente el adjunto, reemplazarlo, insertar X-headers, tags, etc.)
- Método de escaneo inteligente, que no necesite la descarga continua de ficheros de patrones completos, sino que usando la información de sus cabeceras, pueda decidir si usar un patrón u otro de manera más rápida y eficiente.
- Métodos de escaneo basados en patrones tradicionales (toda la información del patrón reside en el endpoint) o escaneo inteligente (la información del patrón reside en una BBDD de reputación centralizada y accesible por los endpoints). La BBDD deberá estar ubicada en la nube y ser actualizada varias veces al día o en el momento de conocerse una nueva amenaza.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 7 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

- Vulnerabilidades no parcheadas: parcheo virtual (bloqueando tráfico que intenten explotar una determinada vulnerabilidad) de las vulnerabilidades tanto de sistema operativo como de aplicativos. Escaneo previo del equipo para identificación de versiones del sistema operativo y de los aplicativos para aplicar únicamente y de manera automática los parches virtuales necesarios para proteger dicho equipo. Reportes individuales por equipos de las vulnerabilidades.
- Motor de reputación Web: detección y bloqueo de Amenazas web permitiendo la personalización de URLs a bloquear/permitir así como ajustar el nivel de agresividad de dicho motor. Dicho motor deberá permitir establecer configuraciones diferentes en función de la ubicación del endpoint (red corporativa u otra).
- Inspección profunda en tráfico web (http/https).
- No es necesaria la funcionalidad de DLP
- Posibilidad de efectuar escaneo de archivos:
  - En tiempo real.
  - Programados.
  - Inmediatos (a demanda).
- Cada método de escaneo debe permitir excluir ficheros del mismo de manera independiente del resto de métodos de escaneo.
- Control de uso dispositivos: control de acceso a dispositivos mediante la asignación de permisos por endpoint, pudiendo configurar los dispositivos que se permiten o no se permiten utilizar al usuario:
  - Dispositivos móviles.
  - Dispositivos de almacenamiento: CD/DVD, unidades de red, dispositivos de almacenamiento USB.
  - Otros: adaptadores Bluetooth, puertos COM y LPT, IEEE 1394, dispositivos de captura de imagen, puertos infrarojos, modems, tarjetas PCMCIA, botón de captura de pantalla.
- Capa de protección para clientes Apple Mac evitando que accedan a sitios maliciosos y que distribuyen malware, incluso si el malware no está dirigido a Mac OS X.
- Aislamiento del endpoint en caso de infección latente ("Out Break"). Con capacidad de configurar umbrales de infección en el endpoint (Virus/Malware, Spyware/Grayware, Firewall blocks, Shared folder Sesion y comunicaciones reportadas como Comand and control), para su posterior notificación y aislamiento de los equipos.
- Actualizaciones programables del producto y de los ficheros de patrones.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 8 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

- Deberán poder establecerse configuraciones y políticas de escaneo distintas en función de la ubicación del endpoint (red corporativa u otra).

5.4 Dimensionamiento

Se ofertarán como mínimo los siguientes elementos:

- Suministro de las licencias necesarias para llegar al mínimo de 2500 exigidas en el presente pliego.
- Suscripción del derecho de actualizaciones de versiones de software, de firmas y de patrones de virus para el servidor de antivirus y los equipos protegidos durante el plazo de garantía del contrato.
- Suscripción de soporte y mantenimiento 24x7 para todas las licencias ofertadas durante el plazo de garantía del contrato.

5.5 Servicios requeridos

5.5.1 Auditoría de la implantación (sólo en caso de mantener la solución del fabricante actual)

En caso de optar por mantener la solución antivirus del fabricante actual, el adjudicatario deberá realizar una auditoría en la que se verifique que la configuración del software de antivirus y de los agentes desplegados en los puestos de usuarios es correcta y cumple con las recomendaciones del fabricante. Esta auditoria deberá tener una duración mínima de dos jornadas de trabajo (una jornada in-situ de revisión y otra de elaboración de informe).

5.5.2 Servicio de implantación y transferencia de conocimientos (sólo en caso de cambio de fabricante de la solución)

En caso de requerirse el despliegue de una nueva solución por haber optado el adjudicatario por ofertar una solución antivirus de distinto fabricante, el adjudicatario será responsable de realizar los siguientes trabajos:

- Todas las pruebas que permitan validar el cumplimiento de todos y cada uno de los requerimientos técnicos de este PPT.
- La migración de la solución actual a la nueva ofertada.
- La transferencia de conocimiento a la Consejería sobre la nueva solución desplegada.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 9 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

Para ello deberán proporcionarse todos los servicios necesarios para realizar la instalación y configuración del producto en la plataforma informática de la Consejería, definición de políticas de seguridad, así como las tareas necesarias para la migración de la configuración de los agentes actuales instalados en los equipos.

El licitador deberá presentar la planificación prevista para la completa ejecución del servicio de implantación y transferencia de conocimientos. Deberá designar un director técnico y jefe de proyecto para la ejecución de los servicios.

Deberá realizarse también una sesión de traspaso de conocimientos del adjudicatario al personal de la Consejería en la que se traten todas las configuraciones y políticas aplicadas sobre el sistema de antivirus, así como todos los procedimientos necesarios para realizar las tareas de mantenimiento de los sistemas. Esta formación tendrá la duración suficiente para que el personal de la Consejería pueda adquirir efectivamente los conocimientos a traspasar, estableciéndose un mínimo de 30 horas.

De esta formación se realizarán al menos dos sesiones en fechas distintas, para facilitar la asistencia del personal técnico. Se deberá impartir en Sevilla en las instalaciones de la Consejería, en las fechas y horarios que indique el Director de Proyecto.

En cualquier caso la instalación y configuración de los elementos objeto de contrato 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.

El plazo máximo para la implantación y la transferencia de conocimientos será de 1 MES a contar desde el díade la firma del contrato, teniendo en cuenta que en dicho plazo todos los puestos de usuario y servidores de la Consejería deberán tener completamente instalada, configurada y activada la nueva solución ofertada.

Deberá proporcionarse toda la documentación técnica del sistema ofertado, así como de las configuraciones instaladas.

El servicio que se requiere del adjudicatario será “llave en mano” para la Consejería, por lo que todos los gastos, materiales y esfuerzos de cualquier índole requeridos para su ejecución serán por cuenta del adjudicatario.

Las intervenciones de los técnicos del adjudicatario se efectuarán ‘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.

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

- Desplazamiento de los técnicos del adjudicatario al lugar de instalación.
- Mano de obra y servicios correspondientes.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 10 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

- Equipamiento y herramientas (tanto hardware como software) necesarias para el correcto desempeño de los trabajos.
- Todos los materiales y componentes requeridos.

Durante el proceso de implantación los puestos que vayan quedando instalados deberán contar con actualizaciones de firmas y patrones de virus.

5.6 Mejoras

Se valorarán como mejora las siguientes especificaciones adicionales a los mínimos requeridos:

- Reducción del plazo de ejecución del contrato hasta 7 días desde el día siguiente al de la firma del contrato.

5.7 Condiciones a las que debe ajustarse la suscripción de actualizaciones y soporte durante el plazo de vigencia de la garantía

Una vez completada la ejecución del contrato, se iniciará el plazo de garantía del mismo durante el cual se deberá proporcionar el mantenimiento y soporte de la solución antivirus ofertada, que incluirá:

- Suscripción del derecho de actualizaciones de versiones de software, de firmas y de patrones de virus para el servidor de antivirus y los equipos protegidos durante el plazo de garantía del contrato.
- Suscripción de soporte y mantenimiento 24x7 para todas las licencias ofertadas durante el plazo de garantía del contrato. La firma adjudicataria asumirá durante el plazo de vigencia de la garantía las obligaciones que se concretan en las siguientes prestaciones.

En la realización de este servicio, los gastos de desplazamientos, dietas, pernoctaciones, etc. que deba realizar el prestador no supondrán coste adicional para la Consejería. En el supuesto caso de que sea necesario recurrir a este servicio, la mano de obra y los componentes necesarios para realizar la sustitución/reparación de los equipos no correrán a cargo de la Consejería.

Asistencia técnica a petición de usuario con el fin de solucionar un mal funcionamiento software de cualquiera de los productos objeto del presente pliego, tanto por razones propias del mismo como consecuencia de cambios en el entorno fisico-lógico en que están instalados.

A efectos de lo anterior, se contemplará un máximo tiempo de respuesta de 4 horas.

La recepción de incidencias deberá poder realizarse por vía telefónica y electrónica (vía correo electrónico y via web) en régimen de 24x7 y siempre con atención en castellano.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 11 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

6 CONDICIONES GENERALES

6.1 Funciones y responsabilidades

La Consejería de Economía, Hacienda y Administración Pública 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 de la Consejería 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 Economía, Hacienda y Administración Pública 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 con la cualificación técnica y profesional necesaria para la ejecución de las tareas asociadas al contrato.

6.2 Plan de proyecto

FASE 1: ejecución del suministro de la solución y de los servicios especificados en el apartado "5.5 Servicios requeridos" del PPT. Esta fase deberá estar finalizada antes de 30 DÍAS desde el día siguiente al de la firma del contrato.

6.3 Acreditación como partner

En caso de que se requiera la sustitución por haber ofertado una solución de distinto fabricante al de la solución actual, la empresa o empresas que vayan a realizar la instalación deberán estar acreditadas como partner por el fabricante del mismo o bien deberán ser el propio fabricante. En caso de que la instalación no la realice el fabricante, la empresa o empresas instaladoras deberán acreditar los siguientes niveles de partner del fabricante del equipo:

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 12 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

Sistema	Nivel de Partner requerido
Antivirus de puesto de trabajo y servidores	Solo se aceptarán los tres niveles de competencia (partner) más altos del fabricante

En caso de no tener alguno de los niveles de partner indicados, la instalación la deberá realizar el propio fabricante.

El adjudicatario deberá completar la siguiente tabla de valoración y adjuntar las certificaciones emitidas por los fabricantes, con carácter previo al inicio del contrato:

Sistema	Fabricante del equipamiento ofertado	Niveles de partner del fabricante (de mayor nivel a menor nivel de competencia)	Empresa que realizará la instalación	Nivel de partner de la empresa instaladora con el fabricante
Antivirus de puesto de trabajo y servidores				

6.4 Documentación entregable del proyecto

Para facilitar a la Dirección del Proyecto tanto las recepciones parciales como la recepción final del proyecto, deberán entregarse 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.

Listado de entregables:

- Documento de suministro en el que aparezca claramente recogido:
  - Denominación comercial de las licencias suministradas
  - Cantidad de licencias suministradas
  - Procedimiento detallado que debe seguirse para la instalación de las licencias
  - Fechas de inicio y de fin del mantenimiento de las licencias suministradas
- Documento de cumplimiento del Esquema Nacional de Seguridad (ENS): documento que relacione las medidas de seguridad del ENS con las funcionalidades del producto suministrado, identificado claramente en qué contribuye cada funcionalidad del producto al cumplimiento de cada medida del ENS.
- En caso de mantener la solución del fabricante actual: documento de resultados de la auditoría de la instalación.
- En caso de cambiar de fabricante de la solución: documentación técnica completa de la solución ofertada, documentación técnica de la implantación y configuraciones realizadas y documentación de la formación impartida.

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 13 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

6.5 Formato de entregables

Toda la documentación del proyecto tendrá que ser entregada en castellano, 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).

6.6 Garantía técnica

Durante el periodo de garantía deberá proporcionarse el servicio de mantenimiento y soporte de la solución suministrada, cuyos requisitos se recogen en el apartado "5.7 Condiciones a las que debe ajustarse la suscripción de actualizaciones y soporte durante el plazo de vigencia de la garantía" de este documento.

El plazo de garantía será el especificado en el Pliego de Condiciones Administrativas Particulares.

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 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", en el Real Decreto 1720/2007 de 21 de diciembre "Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal" y 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 deroga la Directiva 95/46/CE (Reglamento general de protección de datos)".

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 Propiedad intelectual

Toda la documentación generada durante la ejecución de este contrato es propiedad exclusiva de la Consejería de Economía, Hacienda y Administración Pública, sin que el contratista pueda conservarla, ni obtener una copia de la misma o facilitarla a terceros sin la expresa autorización de esta

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 14 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	

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.

6.9 Esquema nacional de seguridad

En cumplimiento con lo dispuesto en el Real Decreto Legislativo 3/2011 de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, el licitador 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.

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. Para ello se requiere la entrega del documento de cumplimiento de ENS descrito en el apartado de "Documentación entregable del proyecto" de este Pliego.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre.

EL JEFE DE SERVICIO DE PRODUCCIÓN

Juan Álvarez Abrio

JUAN ALVAREZ ABRIO		25/07/2018	PÁGINA 15 / 15
VERIFICACIÓN	NJyGwZ7RP36ThF890zt3Q73sjs5GBJ	https://ws050.juntadeandalucia.es/verificarFirma	