Junta de Andalucía
Consejería de Salud y Familias
Consejería de Igualdad,
Políticas Sociales y Conciliación
Agencia de Servicios Sociales
y Dependencia de Andalucía

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR LA CONTRATACIÓN DEL SUMINISTRO Y MANTENIMIENTO DE LA PLATAFORMA DE ANTIVIRUS Y PROTECCIÓN AVANZADA DE LA AGENCIA DE SERVICIOS SOCIALES Y DEPENDENCIA DE ANDALUCÍA

Sumario

1. Antecedentes

La infraestructura tecnológica de la Agencia de Servicios Sociales y Dependencia de Andalucía (en adelante la Agencia) cuenta en sus sistemas de información con numerosos servicios que dan soporte a la gestión de la misma. Entre dichos servicios se encuentran algunos con criticidad máxima ya que son servicios que se prestan ininterrumpidamente las 24 horas del día de los 365 días del año a personas usuarias del servicio en situación de dependencia y a personas mayores de 65 años. Además de los servicios indicados anteriormente, existen servicios troncales para la gestión diaria de la Agencia que no pueden sufrir interrupciones en su operatividad diaria.

La normativa vigente, y en particular el Esquema Nacional de Seguridad (ENS), impone la obligatoriedad de implantar mecanismos que garanticen la disponibilidad de la información y, en concreto, la protección de los sistemas frente a código dañino.

Así, en el artículo 24 del capítulo III (requisitos mínimos) del ENS sobre la continuidad de la actividad, se indica:

> *"Se establecerá un sistema de detección y reacción frente a código dañino."*

Igualmente, en el anexo II de Medidas de Seguridad del ENS, se establece la necesidad de implantar medidas de protección frente a código dañino [op.exp.6]:

> *"Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante."*

Indicando igualmente que:

> *"Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como "spyware", y en general, todo lo conocido como "malware."*

Para dar cumplimento a esta normativa y protegerse frente al código dañino, la Agencia utiliza desde hace varios años el software de Endpoint Protection Platform (EPP) del fabricante Sophos, utilizado para proteger tanto los puestos de trabajo como los servidores y dispositivos móviles. Concretamente, se dispone de 385 licencias para dispositivos móviles, 1200 de puestos de usuario y 100 de servidores.

Este software se encuentra en el catálogo de productos de seguridad[1] del CCN-CERT, como producto aprobado y cualificadado para sistemas de Nivel Medio en la categoría Seguridad en la explotación, en la familia Antivirus/EPP (EndPoint Protection Platform) y en la familia EDR (EndPoint Detection and Response).

[1] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

La acreditación del producto Intercept X Advanced como EPP y EDR se puede consultar en *https://oc.ccn.cni.es/catalogo-productos-stic/listado-de-productos-aprobados/546-intercept-x-advanced-with-edr-2-5-4-beta-10-8-6-2-0-16-beta*.

Los derechos de actualización y el soporte de las licencias adquiridas en su momento por la Agencia del software Sophos expiran en mayo de 2022. Es necesario renovar dichos derechos y el soporte, por los siguientes motivos:

a) Las soluciones de protección ante código dañino, por su propia naturaleza, necesitan actualizarse constantemente para protegerse ante nuevas amenazas.

b) Las nuevas versiones del producto solucionan errores y permiten nuevas funcionalidades que facilitan la gestión y aumentan la protección y disponibilidad de los sistemas.

c) Los parches de seguridad son necesarios para conseguir un nivel adecuado de seguridad. Así lo indica el Esquema Nacional de Seguridad, que en el anexo II establece, entre las medidas del marco operacional, las medidas de mantenimiento [op.exp.4].

d) El soporte especializado telefónico y vía web asociado a las licencias es necesario para poder acometer la resolución de los posibles problemas que puedan aparecer derivados de la utilización del software de antivirus.

Por otro lado, el Esquema Nacional de Seguridad (ENS), en el anexo II de Medidas de Seguridad del ENS, en el apartado 5.3.3 Protección de portátiles [mp.eq.3], se indica:

> *Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.*

Y para la categoría alta, se impone:

> *b) La información de nivel alto almacenada en el disco se protegerá mediante cifrado.*

Para proteger los equipos portátiles, la Agencia utiliza la funcionalidad de cifrado mediante la tecnología bitlocker que incorporan los sistemas Windows. Pero no se dispone de un sistema de gestión centralizada de los equipos cifrados que facilite su gestión y, en caso necesario, la recuperación de las claves de cifrado.

2. Objeto

El objeto del presente pliego es establecer las condiciones que han de regir el suministro para la actualización y adquisición de licencias de software antivirus, así como, del servicio de mantenimiento y soporte experto de la solución, de manera que permita garantizar la protección avanzada de los puestos de trabajo, dispositivos móviles y servidores de la Agencia frente a código dañino.

3. Situación actual

El software de protección EPP (Endpoint Protection Platform) del fabricante Sophos se encuentra desplegado en los puestos de trabajo, dispositivos móviles y servidores de la Agencia desde el año 2018.

Las licencias de las que dispone la Agencia incluyen la funcionalidad Intercept X, que protege contra ataques de ramsonware.

Las licencias y periodo de vigencia de dicho software son las que se muestran en la siguiente tabla:

Descripción	Unidades	Fecha inicio	Fecha fin	Licencia
Sophos EndPoint Protection con Intercept X	1.200	11/05/2021	10/05/2022	L0010533120
Sophos Intercept X for Mobile	385	27/11/2021	26/05/2022	L0007678547
Sophos Intercept X Advance for Server	100	27/05/2021	26/05/2022	L0010978490 /L0010978491

Para garantizar la integración y compatibilidad con el sistema EPP ya desplegado, sin necesidad de desplegar endpoints adicionales ni sustituir los endpoint actuales, se requiere, para los puestos de trabajo y servidores, la ampliación del licenciamiento actual de Sophos.

Adicionalmente, se requiere la adquisición del licenciamiento adicional necesario para la gestión centralizada del cifrado de equipos portátiles, integrada en la consola de gestión centralizada y sin necesidad de instalar agentes adicionales en los equipos.

Como ya se ha indicado, el software EPP de Sophos se encuentra en el catálogo de productos de seguridad del CCN-CERT, como producto aprobado y cualificado para sistemas de Nivel Medio como EPP, es decir, que se ha comprobado que implementan, con cierto nivel de garantía, las funcionalidades de seguridad requeridas por el ENS.

De esta manera, con la renovación y adquisición de nuevo licenciamiento objeto de esta contratación se conseguirá una solución global e integrada para la protección frente a código dañino con las siguientes ventajas:

- Evitar el despliegue de nuevos agentes en la plataforma de puestos, dispositivos móviles y servidores de la Agencia.
- Disponer, con un único agente, de las funcionalidades de EPP y gestión centralizada del cifrado de los puestos de trabajo.
- Mantener la gestión de todos los elementos protegidos desde una única consola de gestión.

4. Especificaciones del suministro y servicios

El suministro de licencias y servicios de soporte debe cubrir al conjunto de dispositivos (puestos de usuario, dispositivos móviles y servidores) y contemplar el conjunto de características que se describen a continuación.

4.1. Características técnicas

Los productos suministrados deben contemplar las siguientes características técnicas:

- Gestión segura centralizada en la nube.

  La gestión de todos los productos suministrados se debe realizar mediante una Consola Central en la nube accesible mediante un navegador de manera segura. La información debe circular cifrada.

- Funcionalidades de antivirus, incluyendo:
  - Antivirus basado en firmas (tradicional).
  - Antiransomware.
  - HIPS (Host Intrusion Prevention System).
  - Control de Aplicaciones: aplicar control sobre qué aplicaciones o categorías de aplicaciones ejecuta un usuario, un grupo de usuarios o una máquina concreta.
  - Control de navegación web.
  - Control de dispositivos: definir qué tipo de dispositivos y qué permisos se otorgan.
  - Control DLP: Definir qué tipo de información se puede mover/copiar el usuario a programas, recursos de almacenamiento, navegadores...
  - Antivirus basado en Deep Learning.
  - Prevención de técnicas de explotación o antiexploit.
  - Prevención de comportamientos maliciosos
  - Prevención de técnicas post-explotación.
  - Prevención de modificación de sector de arranque y del sistema de ficheros.
  - Prevención de ejecución de scripts y herramientas de administración.
- Gestión centralizada de cifrado para los dispositivos móviles Windows indicados.
  - Gestión del cifrado mediante bitlocker.
  - Recuperación de PIN/contraseña de autoservicio.
  - Avisos periódicos a los usuarios para el cambio de contraseñas/PIN.
  - Informes de cumplimiento.
- Debe incluir derechos actualización de :

- Nuevas versiones del producto Software con mejoras o nuevas funcionalidades.
- Hot Fix, es decir, versiones del producto de Software creadas para resolver problemas específicos.
- Parches de seguridad.

La solución debe soportar soportar los siguientes sistemas operativos:

- Windows 7 ,8 ,8.1, 10, 11.
- Windows Server 2008 R2, SBS 2011, 2012. 2012 R2, 2016, 2019.

4.2. Licenciamiento

El licenciamiento objeto de la presente licitación es el siguiente:

- 1500 puestos de usuario con funcionalidades EPP (Central Intercept X Endpoint Advanced).
- 80 Servidores Windows Server EPP (Central Intercept X Advanced for Server).
- 580 dispositivos móviles android con funcionalidades EPP (Central Intercept X for Mobile).
- 70 puestos de trabajo Windows con gestión centralizada de cifrado (Central Device Encryption).
- Soporte extendido para equipos cuyo soporte estándar finalice durante la vigencia del contrato (Central Extended Support for W7/8.1/2008 R2/2012/2012 R2).

4.3. Servicios.

Para garantizar la operatividad, funcionalidad y securización de la solución, se requieren los siguientes servicios:

- Servicios de análisis, configuración y adecuación de la configuración actual:
  - Análisis de la configuración actual. Adecuación a ENS.
  - Análisis de la conveniencia de configuración de servidores para realizar funciones de “Update Cache” y/o “Message Relay”.
  - Propuesta de mejoras.
- Servicio de implantación.
  - Implantación de las propuestas de mejoras.
- Servicio de soporte avanzado sobre los productos objeto de esta licitación.

Las entidades licitadoras deben contar con la certificación Sophos Partner "Platinum" y estar en posesión de la certificación en el Esquema Nacional de Seguridad para proporcionar servicios externalizados en Sistemas de, al menos, nivel medio. El servicio debe ser proporcionado por personal técnico certificado en la solución ofertada.

El detalle de los servicios requeridos se describe a continuación.

4.3.1. Análisis, Configuración y adecuación a ENS

La empresa adjudicataria se responsabilizará de la revisión y modificaciones necesarias en la configuración actual de la plataforma, con el objetivo de mantenerla segura de acuerdo a las buenas prácticas, y en especial, al cumplimiento de los requerimientos del ENS.

En este sentido, la empresa adjudicataria atenderá a las recomendaciones establecidas por el CCN-CERT en su guía de CCN-STIC-1207 Procedimiento de Empleo Seguro Sophos Intercept X Advanced.pdf, en lo relativo a:

- Recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- Recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- Tareas recomendadas a la Agencia para la fase de operación y mantenimiento del producto.

Tras los análisis descritos, la empresa adjudicataria realizará una propuesta de implantación y mejoras para mejorar la protección global de la solución y su adecuación a ENS

4.3.2. Servicios de implantación

Tras los análisis descritos en el apartado anterior, la empresa adjudicataria, junto con el personal técnico de ASSDA, realizará la implantación de:

- Implantación de las propuestas de mejoras.

4.3.3. Servicios de soporte avanzado

El soporte avanzado sobre los sistemas de protección abarcados por esta licitación se realizará:

- En horario 8x5.
- Deberá ser proporcionado por personal técnico certificado en la solución.

Entre las tareas a realizar por dicho soporte se encuentran:

- Realizar las actualizaciones necesarias a la versión recomendada por el fabricante, así como, aplicación de parches de seguridad, conservando las configuraciones y la operatividad de la solución.
- Tareas de análisis y limpieza por infecciones individuales o masivas en los equipos cubiertos por la solución.
- Revisión y comprobación periódica del funcionamiento de la solución, con ajuste de parámetros en caso de ser necesario.
- Asesoramiento experto, así como, cualquier otra consulta sobre la solución adquirida.
- Intermediación con el soporte del fabricante cuando sea necesario.

5. Plazo de ejecución.

Todo licenciamiento suministrado debe contemplar el mantenimiento y soporte durante un año, prorrogable a un año adicional, se debe tener en cuenta la finalización del licenciamiento actual, de manera que el mantenimiento y soporte de todas ellas finalicen en la misma fecha.

El suministro para la actualización y adquisición de las licencias objeto de la presente licitación, deberá ser entregado y activado por la empresa adjudicataria en un plazo máximo de quince (15) días desde la firma del contrato.

6. Confidencialidad y seguridad de la información

La empresa adjudicataria queda expresamente obligada a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación, sin el consentimiento expreso, por escrito, de la Agencia.

Información a la que se le atribuye carácter confidencial:

Tendrá carácter confidencial toda aquella información a la que la entidad adjudicataria tenga acceso con motivo de la ejecución del contrato, particularmente aquella referente a aspectos internos u organizativos de la Agencia, así como a datos de carácter personal. Los datos y productos obtenidos como consecuencia de la ejecución del contrato se considerarán exclusivamente propiedad de la Agencia. Cuando finalice el contrato la entidad contratista devolverá en formato electrónico la documentación generada para el Proyecto en cuestión, así como cualquier otro tipo de información que ésta pueda haber obtenido.

Plazo durante el que la persona contratista deberá mantener el deber de confidencialidad: 5 años

Las proposiciones deberán 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 media, 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.ccncert.cni.es/), así como a las recomendaciones de Andalucía- CERT, como centro especializado en la materia en el ámbito andaluz

7. Tratamiento datos de carácter personal

La entidad contratista, deberá cumplir 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Para ello, y en aplicación de la disposición adicional vigésima quinta de la Ley 9/2017, la contratista tendrá la consideración de encargado del tratamiento.

Asimismo la contratista deberá cumplir la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en virtud de la cual tendrá la obligación de guardar sigilo respecto de los datos de carácter personal a los que tenga acceso en el marco del presente contrato.

Además, deberá cumplir las medidas técnicas y organizativas estipuladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en cuanto no contradigan, se opongan, o resulten incompatibles con la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos.

7. Prevención de Riesgos Laborales

La entidad adjudicataria deberá cumplir con las exigencias de la Ley de Prevención de Riesgos Laborales y su normativa de desarrollo, incluida en la Coordinación de Actividades Empresariales en los supuestos contemplados en el Real Decreto 171/2004, de 30 de enero, por el que se desarrolla el artículo 24 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en materia de actividades empresariales.

8. Presupuesto de licitación

El presupuesto de licitación del presente contrato para el período de un año es de €, 67.439 € IVA excluido y 81.601,19 €, IVA incluido de acuerdo siendo:

- Suministro : 61.541,90 € IVA excluido y 74.465,70 € IVA incluido
- Servicios : 5.897,10 € IVA excluido y 7.135,49 € IVA incluido.

Con el siguiente desglose:

SUMINISTRO			
	Unidades	Precio	Importe sin IVA
Puestos de usuario con funcionalidades EPP (Central Intercept X Endpoint Advanced)	1500	28,45 €	42.675,00 €
Servidores Windows Server EPP. (Central Intercept X Advanced for Server)	80	80,35 €	6.428,00 €
Dispositivos móviles android con funcionalidades EPP. (Central Intercept X for Mobile)	580	17,10 €	9.918,00 €
Puestos de trabajo Windows con gestión centralizada de cifrado. (Central Device Encryption)	70	13,17 €	921,90 €
Soporte extendido para servidores W2008 R2 ,W2012 R2 (Central Extended Support for 2008 R2/2012/2012 R2)	1	1.599,00 €	1.599,00 €
			61.541,90 €

SERVICIOS				
	Perfil	Precio / hora	Horas	Importe sin IVA
Análisis, implantación y soporte avanzado	Gestor de Proyectos (Project Manager)	44,12 €	40	1.764,80 €
	Gestor de Ciberseguridad (CiberSegurity Manager)	42,02 €	60	2.521,20 €
	Especialista en Ciberseguridad (CyberSecurity Specialist)	33,17 €	40	1.326,80 €
	Administrador de Sistemas (System Administrator)	28,43 €	10	284,30 €
				5.897,10 €

Jefatura de Tecnologías de la Información y Comunicaciones

Fdo.: Raúl García León

Secretaría General

Fdo.: Emiliano Cardenal Piris