PLIEGO DE PRESCRIPCIONES TÉCNICAS DE LA EMPRESA PÚBLICA PARA LA GESTIÓN DEL TURISMO Y DEL DEPORTE DE ANDALUCÍA, S.A. PARA LA CONTRATACIÓN DEL SUMINISTRO DE SOFTWARE PARA SERVICIO GESTIONADO EN LA NUBE DE PROTECCIÓN DE DATOS CORPORATIVOS, BASADO EN LA MONITORIZACIÓN DE LAS APLICACIONES, UN SISTEMA DE GESTIÓN Y MANTENIMIENTO DE EQUIPOS Y ACTUALIZACIÓN DE APLICACIONES DE FORMA AUTOMÁTICA Y MONITORIZACIÓN Y AUDITORIA DE DATOS DE INFORMACIÓN PERSONAL IDENTIFICABLE PARA LA EMPRESA PÚBLICA PARA LA GESTIÓN DEL TURISMO Y DEL DEPORTE DE ANDALUCÍA, S.A. MEDIANTE PROCEDIMIENTO ABIERTO DE VALOR ESTIMADO INFERIOR O IGUAL A 100.000 EUROS NO SUJETO A REGULACIÓN ARMONIZADA. LICITACIÓN ELECTRÓNICA (SIREC).

Expediente: C102-04MP-0923-0078

Título: SUMINISTRO DE SOFTWARE PARA SERVICIO GESTIONADO EN LA NUBE DE PROTECCIÓN DE DATOS CORPORATIVOS, BASADO EN LA MONITORIZACIÓN DE LAS APLICACIONES, UN SISTEMA DE GESTIÓN Y MANTENIMIENTO DE EQUIPOS Y ACTUALIZACIÓN DE APLICACIONES DE FORMA AUTOMÁTICA Y MONITORIZACIÓN Y AUDITORIA DE DATOS DE INFORMACIÓN PERSONAL IDENTIFICABLE PARA LA EMPRESA PÚBLICA PARA LA GESTIÓN DEL TURISMO Y DEL DEPORTE DE ANDALUCÍA, S.A.

Código CPV: 48000000-8

PRIMERA.- JUSTIFICACIÓN.

Los servicios y aplicaciones corporativas para la EMPRESA PÚBLICA PARA LA GESTIÓN DEL TURISMO Y DEL DEPORTE DE ANDALUCÍA (a partir de ahora EPGTDA), están soportados por la infraestructura y los Sistemas Informáticos que se encuentran en las sedes de C/ Compañía 40, Málaga, AndaluciaLab (Marbella), Estadio Olímpico puerta M, Sevilla, C/ Cervantes (Úbeda, Jaén), Instalaciones Deportivas de Huelva, Javier Imbroda (Málaga), La Garza (Linares, Jaén), La Cartuja (Sevilla), Centro de Alto Rendimiento (Sevilla), Tiro Olímpico (Camas, Sevilla), Estadio de la Juventud (Granada), Escuela Púbica de Golf de El Toyo (Almería), oficinas de turismo (en todas las provincias de Andalucía) y en concreto a través de su red de comunicaciones y sus Centros de Proceso de Datos (CPD).
Los equipos de usuario se componen de PC's/portátiles con sistemas operativos Windows, de forma destacada, y Mac y Linux para necesidades específicas como diseño y gestión de sistemas, todos en versiones actualizadas.
Debido a este gran parque informático de la empresa, es necesaria la contratación de un servicio de protección completa de equipos, tanto de puestos de trabajo de usuarios como servidores, controlando el comportamiento de cada uno de los procesos ejecutados en cada equipo, además de proveer de los medios de detección y desinfección de malware.

Este servicio permitirá la clasificación de todo el software que se ejecuta en el puesto de trabajo, monitorizará el comportamiento del mismo, asegurará la identificación del software confiable y no confiable y bloqueará la ejecución del software no confiable.

Se debe incluir también un servicio de gestión y mantenimiento de equipos que permitan el control del estado de los equipos, así como poder aplicar políticas e instalar remotamente. Con el fin de fortalecer la seguridad será necesario eliminar las vulnerabilidades de las aplicaciones con un sistema de actualización

SEGUNDA.- OBJETO DEL CONTRATO.

El objeto del presente pliego es la contratación desde el 30 de septiembre de 2023 y para los siguientes 3 años (2023, 2024 y 2025) con la posibilidad de una prórroga por los 2 años siguientes

(2026, 2027) de un servicio de protección completa de 400 equipos, puestos de trabajo de usuarios y servidores, controlando el comportamiento de cada uno de los procesos ejecutados en el parque informático de la EPGTDA, además de proveer de los medios de detección y desinfección de malware.
Este servicio permitirá la clasificación de todo el software que se ejecuta en el puesto de trabajo, monitorizará el comportamiento del mismo, asegurará la identificación del software confiable y no confiable y bloqueará la ejecución del software no confiable.
Se debe incluir también un servicio de gestión y mantenimiento de equipos que permita el control del estado de los equipos, así como poder aplicar políticas e instalar remotamente.
Con el fin de fortalecer la seguridad será necesario eliminar las vulnerabilidades de las aplicaciones con un sistema de actualización

TERCERA.- CARACTERÍSTICAS TÉCNICAS.

Las características técnicas de la solución ofertada deben ser las siguientes:

ACTIVOS A PROTEGER
La solución deberá ser capaz de proteger al menos 400 equipos (CPU)

UBICACIÓN PLATAFORMA
Con el fin de reducir los costes de mantenimiento y explotación de la solución, no deberá ser necesario el uso de una plataforma interna, se precisa una solución basada en cloud. Es requisito mínimo que la plataforma donde se aloje la infraestructura se encuentre fuera de nuestras instalaciones y operada por el fabricante de la solución en un modelo cloud, en el que no haya un inconveniente en el crecimiento y escalabilidad de la plataforma, asegurando que, independientemente del número de nodos de la instalación, la plataforma funcione en el mismo nivel de eficiencia.
La ubicación de la plataforma debe estar alojada en la Unión Europea.
Existen nodos que están distribuidos por diferentes sedes e incluso en movilidad por lo cual estos aprovecharan la disponibilidad de la infraestructura cloud para que estén integrados de forma completa en la configuración y actualización de la solución.
La plataforma de gestión debe cubrir los principales niveles de certificación como son: ISO 27001 y se valorara positivamente cualquier otra certificación que disponga la infraestructura.

COMPONENTES DEL SERVICIO
Infraestructura Cloud
El adjudicatario proveerá, desde la nube, el conjunto de servidores, bases de datos y procesos de tratamiento de la información relacionada con el servicio. Los procesos capturados de los clientes serán tratados en la nube de tal forma que el impacto sobre los sistemas corporativos sea mínimo.
La gestión de los equipos se realizará desde la nube permitiendo que puedan ser gestionados equipos en diferentes ubicaciones e incluso en movilidad.
Agente a desplegar en los equipos
El agente desplegado permitirá la comunicación y gestión de tanto la protección de antivirus tradicional, así como de la protección de procesos desconocidos y la gestión y conexión remota a los equipos.
Recogerá la información correspondiente a los eventos y los componentes que los producen, sin recopilar información, ni documentos de usuario. El impacto sobre los dispositivos del parque deberá ser menor al 5 % de rendimiento de la CPU, memoria y disco.
El agente debe ser capaz de proteger equipos de sobremesa y portátiles con los siguientes sistemas operativos:

- Desde Microsoft Windows XP SP3 hasta Microsoft Windows 11.

Deberá proteger equipos servidores con las versiones de sistema operativo:

- Desde Microsoft Windows 2003 hasta Microsoft Windows 2019.

La desinstalación de la protección deberá protegerse mediante contraseña.
La solución debe poder desplegarse de manera silenciosa mediante políticas de Directorio Activo de Microsoft y usando la propia consola.

Consola Web
El adjudicatario proporcionará un interfaz en el que se puedan consultar datos en tiempo real, descargar informes/alertas, acceder a la configuración y políticas y disponer de las actualizaciones de los agentes.
Los administradores del servicio podrán gestionar desde una única consola y de manera centralizada, mediante cualquier navegador web la seguridad y productividad de todas las estaciones de trabajo y servidores Windows incluso ordenadores portátiles y oficinas remotas.
PROTECCIÓN
La protección solicitada se dividirá en varias partes:

- Endpoint Protection Platform (EPP)
- Remote Monitoring & Management (RMM)
- Sistema de actualización de software

Todos los componentes del servicio deben estar integrados en un solo agente y una sola solución. No se permitirá el uso de diferentes componentes, con el fin de conseguir una protección contra amenazas desconocidas en la que colabore el antivirus con la monitorización hardware y software de los equipos
Endpoint Protection Platform
Se requiere una solución de EPP (Endpoint Protection Platform) con las siguientes funcionalidades:

- Antivirus para archivos, correo y web. Permitiendo la detección y desinfección de cualquier tipo de amenaza y detección de malware por comportamiento. El correo detectara tanto en SMTP como en POP3. En cuanto a la protección web se detectarán los intentos de acceso a páginas web que contengan elementos maliciosos, bloqueándolos.
- Firewall personal gestionado en local o de forma centralizada desde la consola web. Debe permitir:
    - Bloquear las conexiones entrantes y/o salientes de las aplicaciones que desee
    - Prevención de intrusiones
    - Crear reglas de firewall para permitir/denegar el tráfico en sentido entrante/saliente de las máquinas que quiera para los protocolos/puertos que desee.
- Bloqueo de todos los dispositivos o dispositivos específicos (unidades de almacenamiento extraíbles, dispositivos de captura de imágenes, unidades de CD/DVD, módems USB, Bluetooth, etc.), impidiendo la entrada de malware y fugas de información. Permitiendo la definición de diferentes acciones para cada tipo de dispositivo (bloqueo, acceso, lectura/escritura).
- Bloqueo de acceso a páginas web no deseadas. Deberá ser posible configurar esta protección basada en categorías, aunque se podrán también añadir listas blancas y negras de sitios y dominios permitidos.

Remote Monitoring & Management
Se requiere una solución de tipo RMM (remote monitoring and management) para conseguir los siguientes objetivos:

- Obtener información centralizada de hardware y software.
- Control de licencias utilizado
- Capacidad de hacer filtros por la información obtenida en el inventario
- Registro de cambios producidos en el equipo a nivel de hardware o software.
- Monitorización de procesos, servicios, memoria, CPU, registro, tamaño de archivos o carpetas
- Posibilidad de crear nuevos monitores personalizados
- Monitorización de dispositivos de red.
- Capacidad de realizar tareas de forma automática cuando se produzca un hecho determinado en un monitor.
- Gestión de parches de Microsoft, independientemente de donde se encuentre el equipo.
- Instalación, desinstalación y parcheo de software de terceros.
- Ejecución remota de scripts para automatizar tareas
- Control remoto a equipos conectados a Internet independientemente de donde se encuentren.
- Sistema de comunicación con el usuario mediante Chat.

Todas estas funcionalidades estarán integradas como parte de un solo agente y permitirá tanto la gestión como el control remoto.

Patch Management
Para conseguir un correcto nivel de seguridad es necesario mantener las aplicaciones del parque de equipos con las últimas actualizaciones. Actualmente no se puede dejar la seguridad en la actualización del sistema operativo exclusivamente, se calcula que más del 80% de las vulnerabilidades corresponden a software de terceros.
Por este motivo se requiere un sistema de actualización de aplicaciones con los siguientes requisitos:

- Aplicación de actualizaciones de sistema operativo Microsoft Windows.
- Aplicación de actualizaciones de software de terceros como son Adobe, Oracle, Google, etc.
- Posibilidad de despliegue en tiempo real
- Despliegue programado
- Información gráfica que muestre el estado del parque
- Filtros de búsqueda de parches por actualización o por equipo
- Control sobre el reinicio de los equipos
- Control de las dependencias entre parches
- Cacheo de las actualizaciones para compartirlas localmente.
- Registro de las acciones relacionadas con las actualizaciones.
- Posibilidad de generar reglas para el parcheo automático, según su criticidad, fabricante y software.
- Detección de aplicaciones fuera del ciclo de actualización del fabricante (EoL).

ESQUEMA NACIONAL DE SEGURIDAD
La solución obligatoriamente tiene que estar incluida en el "Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación." (CPSTIC) Publicado por el CCN (Centro Criptográfico Nacional), dentro de la familia de protección del Puesto de Trabajo como CUALIFICADO ENS Alto tanto en la categoría de EndPoint como en la de EDR. La Tecnología Cloud Pública es obligatoria que tenga la certificación de conformidad frente al ENS, de categoría alta.
INFORMACIÓN
El sistema debe generar información forense relacionada con cada equipo de tal forma que pueda ser explotada posteriormente. El sistema deberá incluir informe por amenaza detectada en la que se correlacione las acciones que ha hecho el proceso o en el contexto que ha estado envuelto. Por ejemplo, si ha sido descargado de Internet o ha sido extraído de un fichero comprimido. Se valorará un entorno amigable y fácil de seguir, sin exigir grandes conocimientos de amenazas avanzadas. Además, debe incluir informes de estado de las protecciones, de las detecciones de malware y algún informe ejecutivo con el resumen de la información global.
Los informes se deben de poder obtener de forma inmediata con los datos en tiempo real y también de forma periódica por correo electrónico y en diferentes formatos para su posterior tratamiento.
SOPORTE TÉCNICO 24x7x365
Se establecerá el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento en todos los puestos y servidores de la organización. Mediante:

- Servicio de soporte ofrecido por el fabricante por teléfono en castellano.
- Service Packs y hotfixes: Acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus, …
- Soporte técnico vía email 24x7x365, por técnicos certificados en la solución implementada
- Acceso a análisis online de virus ocultos
- Acceso ilimitado al Helpdesk: sin límite de incidencias

CUARTA.- LUGAR DE REALIZACIÓN DE LOS TRABAJOS.

Los trabajos de mantenimiento se podrán realizar en las instalaciones de la empresa adjudicataria, vía telefónica o por correo electrónico.
Por petición del Responsable del Contrato y para la óptima realización del contrato, existe la posibilidad de que algunos trabajos se deban desarrollar en instalaciones o edificios de la EPGTD, en tal caso, los trabajos se realizarán en las sedes de C/Compañía 40, Málaga o Estadio Olímpico Puerta M, Sevilla.

QUINTA.- PLANIFICACIÓN Y EQUIPO DE TRABAJO.

Turismo y Deporte de Andalucía designará un responsable de los trabajos cuya función será, con carácter general, la supervisión de la correcta realización de los mismos, la aprobación de la planificación de los trabajos y su seguimiento.
Asimismo, la empresa adjudicataria designará una persona que actúe como representante de la misma ante Turismo y Deporte de Andalucía para resolver cualquier consulta o incidencia que pudiera surgir en el desarrollo de los trabajos a realizar.
Durante la realización de los trabajos objeto del contrato, Turismo y Deporte de Andalucía podrá efectuar cuantas sugerencias y propuestas se consideren necesarias para el buen fin de la realización de los trabajos.

SEXTA.- CONTROL DE LOS TRABAJOS.

Turismo y Deporte de Andalucía designará un responsable de los trabajos, cuya función será con carácter general, la supervisión de la correcta realización de los mismos, la aprobación de la planificación de los trabajos, y su seguimiento.
Asimismo, la empresa adjudicataria designará una persona que actúe como representante de la misma ante Turismo y Deporte de Andalucía para resolver cualquier consulta o incidencia que pudiera surgir en el desarrollo de los trabajos a realizar.
El control del proyecto se realizará por la dirección de Turismo y Deporte de Andalucía a través de la persona responsable designada, y se hará de forma sistemática, a lo largo del desarrollo del mismo, para asegurar el cumplimiento de objetivos básicos y garantizar la calidad e integridad de los trabajos.

SÉPTIMA.- SEGURIDAD.

Las ofertas se presentarán conformes a la normativa que sobre el Marco de Seguridad de las Tecnologías de la Información haya dictado la Junta de Andalucía.

OCTAVA.- GESTIÓN DE USUARIOS Y CONTROL DE ACCESO.

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, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del 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, 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, quien recibe derechos de acceso y del tipo que son.
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, de acuerdo a las consideraciones establecidas en el anexo II del ENS.
Se exige que cualquier adaptación que afecte al módulo de gestión de usuarios (roles, gestión de identificador de usuario y contraseña, etc.) deberá respetar todas 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.

NOVENA.- PROPIEDAD INTELECTUAL DEL RESULTADO DE LOS TRABAJOS.

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de la Junta de Andalucía, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la Junta de Andalucía. Específicamente todos los derechos de explotación y titularidad de las

aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente a la Junta de Andalucía.

DÉCIMA.- SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS.

La empresa adjudicataria se compromete a salvaguardar la disponibilidad, confidencialidad e integridad de los datos a los que tenga acceso.
La empresa adjudicataria en relación con ficheros que contengan datos de carácter personal a los que pudiere tener acceso se compromete al cumplimiento con lo establecido en el Reglamento General de Protección de Datos y la normativa aplicable.

UNDÉCIMA.- GARANTÍA Y MANTENIMIENTO.

El periodo de garantía de los trabajos, comprenderá los 3 años de la ejecución del servicio. Durante dicho periodo se garantizará el mantenimiento de los trabajos realizados. Esta garantía cubre la totalidad de las prestaciones humanas y materiales requeridas para la subordinación de los defectos observados y éstas se realizarán, sin devengo económico alguno, en las mismas condiciones en que se prestaron originariamente los servicios.

DUODÉCIMA.- COSTE

El coste máximo del servicio es de 36.154,80 euros, IVA incluido, 29.880,00 euros IVA no incluido, que serán íntegramente destinados al objeto de los servicios.
Los costes desglosados máximos de los servicios solicitados por 3 años son:

Servicio	**Cantidad**	**Precio Unitario (sin iva)**	**Coste total (sin iva)**	**Coste total (con iva)**
Endpoint Protection Platform Monitoring & Management	400	51,00€	20.400,00€	24.684,00€
Patch Management	400	23,70€	9.480,00€	11.470,00€
TOTALES		**74,70€**	**29.880,00€**	**36.154,80€**

Málaga, a 25 de septiembre de 2023