ACUERDO DE INICIO PARA LA CONTRATACIÓN DEL SUMINISTRO DE SUSCRIPCIÓN A UNA LICENCIA CORPORATIVA PARA LA AMPLIACIÓN DE LAS FUNCIONALIDADES DE LA SOLUCIÓN PARA LA DETECCIÓN Y RESPUESTA A CIBERINCIDENTES EN EQUIPO FINAL DE LA AGENCIA DIGITAL DE ANDALUCÍA PARA EL SERVICIO ANDALUZ DE SALUD, EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA. FINANCIADO POR LA UNIÓN EUROPEA-Next Generation. CC 2114/2024 (Nº SIGLO 0994/2024).

ANTECEDENTES

PRIMERO.- La Agencia Digital de Andalucía (en adelante ADA), a través del expediente CONTR. 2022/816345 "SUMINISTRO DE LICENCIAS POR SUSCRIPCIÓN Y SERVICIO DE SOPORTE ASOCIADO DE UNA SOLUCIÓN PARA LA DETECCIÓN Y RESPUESTA A CIBERINCIDENTES EN EQUIPO FINAL (EDR)" contrató la suscripción a una herramienta basada en la tecnología del fabricante CrowdStrike de protección de endpoints (equipos finales) de nueva generación (soluciones EDR – Endpoint Detection and Response) y servicios asociados. El pliego de prescripciones técnicas de dicho contrato detalla que "el alcance del contrato lo constituyen todos los organismos de la Administración de la Junta de Andalucía, sus entidades instrumentales, los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía y otras instituciones de la Junta de Andalucía previa suscripción de un convenio" quedando, por tanto, dentro del alcance, los equipos finales del Servicio Andaluz de Salud (en adelante SAS).

La actual plataforma tecnológica consta de los siguientes módulos y capacidades:

- **Falcon Insight (EDR):** habilita la extracción de telemetría de procesos de los endpoints (más de 460 eventos de sistema) y su almacenamiento en el tenant del cliente en la nube de CrowdStrike. Esta información se almacena en el modelo de base de datos de CrowdStrike (Threat Graph) con distintos periodos de retención en función de las necesidades. Esta telemetría enriquecida permite correlacionar la información de toda la base instalada y la aplicación de motores de detección basados en machine learning en cloud facilitando la detección de eventos de especial complejidad, así como la aplicación de medidas de análisis, investigación, contención y respuesta globales. Adicionalmente, se habilita la posibilidad de realización de búsqueda activa de amenazas por parte del Cliente (threat hunting) sobre la información de telemetría desde la propia consola cloud. Falcon Insight proporciona visibilidad integral continua sobre toda la base instalada de endpoints habilitando capacidades de detección, respuesta y análisis forense para asegurar que no se pierde información de diagnóstico y que las posibles brechas de seguridad son detenidas en tiempo y forma. Mediante la monitorización continua de la actividad de procesos de los endpoints, permite la aplicación de medidas de detección

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	JOSE ANTONIO MIRANDA ARANDA	14/10/2024
VERIFICACIÓN	Pk2jmWTCRJW79W6GRHLTKC9TFZMQK7	PÁG. 1/6

y protección en tiempo real en el momento en el que se producen los intentos de intrusión.

- **Falcon Threat Graph:** recopila la telemetría enriquecida de los endpoints con Falcon Insight (EDR) y realiza la custodia en la plataforma Falcon (sobre el motor de base de datos Threat Graph de CrowdStrike), facilita las tareas de análisis desde la propia consola de administración, facilitando el lanzamiento de queries y consultas sobre la información de telemetría, lo que permite a los equipos de seguridad investigar, contener y responder a los ataques más sofisticados. Mediante el mapeo de los incidentes con MITRE (MITRE Adversarial Tactics, Techniques, and Common Knowledge – ATT&CK), la plataforma proporciona una capacidad para entender los ataques más complejos de un vistazo.
- **Falcon Device Control:** proporciona capacidades de securización, control y trazabilidad sobre dispositivos USB. Considerando que este tipo de dispositivos son continuas fuentes de entrada de atacantes y de exfiltración de información, Falcon Device Control proporciona capacidades de control granular sobre las operaciones permitidas con los dispositivos USB, garantizando a los administradores de seguridad que únicamente se usan los dispositivos USB autorizados.
- **Falcon Firewall Management:** proporciona capacidad de gestión centralizada de los firewalls de hosts permitiendo la definición, aplicación y control de políticas globales.
- **Falcon Fusion (SOAR):** proporciona capacidades de automatización y orquestación de procesos vinculados a eventos de telemetría o detección. Con Falcon Fusion, integrado en la plataforma Falcon, pueden automatizarse procesos de operación de la seguridad de forma sencilla, reduciendo drásticamente el esfuerzo de operación.
- **Falcon Discover (Descubrimiento y Gestión de la Configuración):** proporciona capacidades de descubrimiento, análisis y gestión de la configuración de los activos. A partir de la información de telemetría extraída de los endpoints, la plataforma Falcon, desde un punto de entrada único muestra información significativa relacionada con la configuración de los distintos endpoints mostrando en tiempo real información relativa a los recursos hardware de los equipos, aplicaciones instaladas, aplicaciones en uso, monitorización de cuentas de usuario, detección de aplicaciones no corporativas (shadow IT), dispositivos no gestionados, etc.
- **Falcon Spotlight (Gestión de Vulnerabilidades):** proporciona capacidades de descubrimiento, análisis y gestión de vulnerabilidades de sistema operativo y aplicaciones residentes den los endpoints. A partir de la información de telemetría extraída de los endpoints, la plataforma Falcon, desde un punto de entrada único muestra información significativa relacionada con las vulnerabilidades detectadas en los endpoints y propone itinerarios recomendados de parcheo de cara a reducir la superficie de exposición del Organismo. Adicionalmente a la información relacionada con la criticidad de la vulnerabilidad, indica si existe evidencia de explotación a nivel mundial de esa vulnerabilidad, siendo esta una información muy significativa de cara a modificar una política de parcheo corporativa.
- **Falcon ITP (Identity Threat Protection):** proporciona capacidades de detección y prevención en tiempo real contra ataques basados en el uso de identidades (credenciales corporativas) y

Es copia auténtica de documento electrónico

vulnerabilidades de protocolos de autenticación.

- **Falcon Sandbox:** proporciona capacidades de detección avanzadas basada en análisis de comportamiento tras ejecución de ficheros en entorno aislado de detonación (Sandbox) en cloud.
- **Falcon Overwatch:** proporciona un servicio 24x7x365 de threat hunting (búsqueda de amenazas) gestionado y especializado sobre la plataforma Falcon. Overwatch incluye la componente de análisis humano realizado directamente por los analistas de seguridad expertos de CrowdStrike, permitiendo detectar comportamientos anómalos correspondientes a ataques diseñados para evadir las distintas tecnologías de seguridad.

No obstante, el SAS requiere de otras funcionalidades que no quedaron cubiertas con dicha contratación y que se deben agregar a las capacidades de la herramienta adquirida por la ADA.

SEGUNDO.- A efectos de atender esas necesidades no cubiertas, el Servicio de Informática del SAS, emite memoria justificativa, de fecha 14 de octubre de 2024 en la que expone la necesidad de la contratación definida en el encabezamiento de esta resolución, ya que es preciso para poder analizar comportamientos de usos complejos tanto de equipos finales (servidores, puestos de usuario, equipamiento de red,…), como de los usuarios que utilizan el equipamiento y las aplicaciones corporativas a las que se conectan, con el fin de detectar comportamientos indebidos, intrusos o ataques de ciberdelincuentes, reduciendo los riesgos para la organización y permitiendo un mejor control y vigilancia de los puntos débiles de los distintos sistemas. En caso de no contar con esta herramienta, o bien la información de las distintas vulnerabilidades y amenazas no estará disponible o lo estará en silos no integrados con la herramienta EDR adquirida por la ADA, por lo que las alertas e investigaciones que llevan a cabo los técnicos de seguridad serán mucho más lentas y pobres. Por tanto, los sistemas estarían más expuestos a los ataques de los ciberdelincuentes al no contar con la necesaria telemetría integrada que permitiese la detección de ataques sofisticados, pudiendo poner en riesgo los sistemas informáticos del SAS y, por ende, la continuidad asistencial y la seguridad del paciente.

TERCERO.- El objeto del contrato, tal como se ha definido anteriormente, lo constituye el suministro de la suscripción, durante cuarenta y ocho meses, a una licencia corporativa para ampliar las funcionalidades de la solución de la Agencia Digital de Andalucía de la Junta de Andalucía, para la detección y respuesta a ciberincidentes en equipo final (EDR por sus siglas en inglés), para los sistemas que dan servicio al Servicio Andaluz de Salud, asegurando que este producto tiene cubiertos sus requisitos en cuanto a actualización a nuevas versiones del software, acceso a parches y hotfixes, y resolución de las incidencias del producto.

CUARTO.- En la memoria justificativa del expediente, se indica que el mismo, se financiará por el Mecanismo de Recuperación y Resiliencia de la Unión Europea, establecido por el Reglamento (UE)

Es copia auténtica de documento electrónico

2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un Instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, y regulado según Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia. Concretamente, se incluye en el componente 11 denominado "Modernización de las Administraciones públicas", Inversión 3 "Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las CCAA y las EELL."

En relación a esta fuente de financiación, se recoge en la memoria justificativa del expediente el cumplimiento de los requisitos y condiciones derivados de la aplicación de este mecanismo, tal como se expone a continuación:

1.- Plan de medidas antifraude.

" *Por todo lo expuesto, este contrato queda sujeto al Plan de Medidas Antifraude, aprobado por la Comunidad Autónoma de Andalucía, con la finalidad de dar cumplimiento a las obligaciones impuestas en el artículo 22 del Reglamento UE 2021/242 del Parlamento Europeo y del Consejo , de 12 de febrero de 2021…".*

2.- Evaluación de riesgo de fraude y corrupción

La memoria indica al respecto, que se ha procedido a la cumplimentación de los Anexos II y VII del Plan de Medidas Antifraude.

3.- Comprobación ausencia de conflictos de intereses.

La memoria indica que se acompañan las declaraciones de ausencia de conflictos de interés indicadas en la Instrucción 2/2023 de la Dirección General de Contratación, en relación con los contratos públicos financiados con fondos procedentes del mecanismos de recuperación y resilencia en ejecución del plan de recuperación, transformación y resilencia.

4.- Doble financiación a la misma ayuda:

Se ha verificado la ausencia de doble financiación del expediente de contratación actual, así como se ha corroborado la no existencia de ninguna otra ayuda de Estado destinada a financiar la actuación objeto del presente contrato….

QUINTO.- El presupuesto base de licitación del expediente, asciende a CUATRO MILLONES OCHOCIENTOS CUARENTA MIL EUROS (4.840.000 €), en los que están incluidos OCHOCIENTOS CUARENTA MIL EUROS (840.000 €), correspondientes al 21% del IVA.

Es copia auténtica de documento electrónico

SEXTO.- El valor estimado del contrato, IVA exento, asciende a CUATRO MILLONES DE EUROS (4.000.000 €):

CONCEPTO	PRESUPUESTO BASE DE LICITACIÓN (IVA EXCLUIDO)	TOTAL
Suscripción de una licencia corporativa para ampliar funcionalidades del EDR corporativo de la Agencia Digital de Andalucía	4.000.000,00 €	4.000.000,00 €
TOTAL, VALOR ESTIMADO (IVA no incluido)		4.000.000,00 €

SEPTIMO.- El expediente se financiará con cargo a las partidas presupuestarias que a continuación se indican correspondientes a los fondos aportados dentro del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea- Next Generation EU. Son las siguientes:

- 1331.18.0880 G/41C/60906/00
  4.000.000,00 € para el cumplimiento del Objetivo 4 del Plan de Atención Primaria y Comunitaria, que proviene del Componente 11, Inversión 3 del Mecanismo de Recuperación y Resiliencia de la Comisión Europea (C11I3: Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las CCAA y las EELL).

- 1331.06.0880 G/41C/60906/00
  840.000,00 € de crédito autofinanciado, correspondiente al IVA de la contribución de la fuente de financiación MRR.

CONCEPTO	Fondo	Partida presupuestaria	2025	TOTAL
Suscripción de licencia corporativa	MR04110301	1331.18.0880 G/41C/60906/00	4.000.000 €	4.000.000 €
21% de IVA	Autofinanciada	1331.06.0880 G/41C/60906/00	840.000 €	840.000 €
TOTAL, IVA INCLUIDO			**4.840.000 €**	**4.840.000 €**

OCTAVO.- La duración del contrato será de un mes, a contar desde su formalización.

NOVENO.- El procedimiento para la adjudicación del contrato es el procedimiento abierto, con varios criterios en base a la mejor relación calidad-precio, de acuerdo con los artículos 131, 145 y 146 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (BOE nº 272 de 9 de noviembre).

Es copia auténtica de documento electrónico

Vista la documentación del expediente, constando justificación de la naturaleza y extensión de las necesidades a cubrir mediante el objeto del contrato, la idoneidad de su contratación para los fines del Servicio Andaluz de Salud, así como de la conveniencia de la utilización del procedimiento, y de los criterios de adjudicación tal como se establece en el artículo 116.4 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, procede acordar el inicio del expediente de contratación.

Por lo expuesto, en virtud de lo establecido en el artículo 14 del Decreto 198/2024, de 3 de septiembre, por el que se establece la estructura orgánica de la Consejería de Salud y Consumo (BOJA extraordinario nº 16 de 4 de septiembre de 2024), y en virtud del artículo 3 de la Resolución de 20 de enero de 2022, de la Dirección Gerencia del Servicio Andaluz de Salud, por el que se delegan competencias en diferentes órganos (BOJA nº 22 de 2 de febrero de 2022),

ACUERDA:

PRIMERO.- Autorizar el inicio del expediente de contratación administrativa para la contratación del suministro de la **suscripción a una licencia corporativa para la ampliación de las funcionalidades de la solución para la detección y respuesta a ciberincidentes en equipo final de la Agencia Digital de Andalucía para los sistemas que dan servicio al Servicio Andaluz de Salud, en el marco del Plan de Recuperación, Transformación y Resiliencia, CC 2114/2024 (nº siglo 0994/2024),** por procedimiento abierto y tramitación ordinaria, siendo el presupuesto base de licitación de **CUATRO MILLONES OCHOCIENTOS CUARENTA MIL EUROS (4.840.000 €)**, en los que están incluidos **OCHOCIENTOS CUARENTA MIL EUROS (840.000 €)**, correspondientes al 21% del IVA, con un plazo de ejecución del contrato de un mes desde su formalización.

SEGUNDO.- Aprobar el Pliego de Prescripciones Técnicas Particulares, de conformidad con lo dispuesto en el artículo 124 de la citada Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

TERCERO.- Declarar la improcedencia de la revisión de precios, por no cumplirse los requisitos previstos en el artículo 103 de la LCSP, así como en la Ley 2/2015, de 13 de marzo, de Desindexación de la Economía Española y el Reglamento de desarrollo de la misma, aprobado por RD 55/2017, de 3 de febrero.

EL DIRECTOR GENERAL DE GESTIÓN ECONÓMICA Y SERVICIOS

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN		
FIRMADO POR	JOSE ANTONIO MIRANDA ARANDA	14/10/2024
VERIFICACIÓN	Pk2jmWTCRJW79W6GRHLTKC9TFZMQK7	PÁG. 6/6