

Exp.: **A/SUM-045459/2024**

*Este documento se ha obtenido directamente del original, que contenía todas las firmas auténticas, y se han ocultado los datos personales y los códigos que permitían acceder al original.*

**Unidad administrativa:**  
DIVISIÓN DE CONTRATACION

Orden 228/2024 de la Consejería de Digitalización, por la que se dispone el inicio del expediente de contratación titulado: "SUMINISTRO, CONFIGURACIÓN E INSTALACIÓN AVANZADA DE UN SISTEMA DE CONTROL DE SEGURIDAD DE EQUIPOS CONECTADOS A LA RED DE COMUNICACIONES DE LOS CENTROS DE ATENCIÓN PRIMARIA DEL SERMAS" CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA - FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU" (C11.I03.P14.S13)" y declarar su tramitación urgente.

De conformidad con lo que establece los artículos 28, 116 y 119 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, y en uso de las atribuciones que me han sido conferidas por las disposiciones vigentes,

### RESUELVO

**Primero.** - Autorizar el inicio del expediente de contratación titulado "SUMINISTRO, CONFIGURACIÓN E INSTALACIÓN AVANZADA DE UN SISTEMA DE CONTROL DE SEGURIDAD DE EQUIPOS CONECTADOS A LA RED DE COMUNICACIONES DE LOS CENTROS DE ATENCIÓN PRIMARIA DEL SERMAS" CON CARGO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA - FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU" (C11.I03.P14.S13)" , cuyo presupuesto base de licitación asciende a 4.692.868,96 euros.

**Segundo.** - Declarar la tramitación urgente del expediente mencionado conforme a lo expuesto en los antecedentes.

De conformidad con lo establecido en los artículos 28 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y 73 del Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas, a continuación, se exponen la naturaleza y extensión de las necesidades que pretenden cubrirse mediante el contrato proyectado, así como la idoneidad de su objeto y contenido para satisfacerlas.

Según se dispone en el Decreto 76/2023, de 5 de julio, del Consejo de Gobierno, por el que se establece la estructura orgánica básica de las Consejerías de la Comunidad de Madrid, y según Decreto 261/2023, de 29 de noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Digitalización, corresponde a la Dirección General de Salud Digital (DGSD): "La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Servicio Madrileño de Salud, de acuerdo con las necesidades explicitadas por este último, así como la tramitación electrónica en el Servicio Madrileño de Salud" y "La provisión y gestión de los servicios y equipamientos informáticos sanitarios del Servicio Madrileño de Salud, en colaboración con el Servicio Madrileño de Salud".

Desde el Ministerio de Sanidad se potencia la estrategia de salud digital y a ello se orientan diversas iniciativas, entre ellas los fondos MRR para la Atención Primaria, potenciando la seguridad ante el aumento de ciberataques dirigidos contra el sector sanitario español, con graves consecuencias como el cese total o parcial de su actividad. Las áreas susceptibles de ataques de los centros sanitarios se amplían constantemente por el incremento del número de interfaces de comunicación y dispositivos médicos conectados que se utilizan, a esta mayor superficie de ataque, se añade una deficiente segmentación de la red, controles de acceso débiles y dependencia de sistemas obsoletos.

Exp.: **A/SUM-045459/2024**

*Unidad administrativa:*  
**DIVISIÓN DE CONTRATACION**

En este sentido, surge la necesidad de garantizar la ciberseguridad en un entorno con un gran Número de dispositivos médicos de naturaleza heterogénea conectados a la red corporativa y manejando información médica de los pacientes

Por otro lado, los Centros de Operaciones de Seguridad (SOC) están ya consolidados en Tecnología de la información (TI). Sin embargo, la realidad de los centros sanitarios o de los sistemas industriales es distinta. Igualmente, cada vez hay más dispositivos conectados a la red y, por tanto, sometidos a amenazas de ciberseguridad, pero los ataques a este tipo de dispositivos son susceptibles de causar pérdidas de vidas humanas o daños en las mismas.

Esto hace que estos entornos es preciso asegurar la continuidad del servicio a prestar, además de preocuparse de la confidencialidad, integridad, disponibilidad o autenticidad de la información.

Un Centro de Operaciones de Seguridad que deba gestionar este tipo de dispositivos (IoT, OT o IoT en general) sigue debiendo gestionar las alertas de seguridad, respondiendo a incidentes, conocer y gestionar las vulnerabilidades o recuperar la operativa. Sin embargo, las herramientas actuales difieren.

El SOC no tiene, en muchas ocasiones, documentación sobre estos dispositivos, sistemas o procesos, y para asegurar la continuidad del servicio no puede ser intrusivo, donde se requieren disponer de mejores herramientas para clasificar los activos. El objetivo final es poder identificar los riesgos derivados de esos equipos conectados y establecer las medidas de seguridad necesarias que eviten una exposición innecesaria, como consecuencia de esos riesgos, especialmente por no contar con software o configuraciones actualizaciones.

El ámbito de actuación de este contrato abarcará la implantación y soporte de un sistema de control y seguridad de equipos conectados, enfocado en el ámbito sanitario. Este sistema estará encargado de la captación de los datos relevantes de comportamiento de los dispositivos ubicados en las redes sanitarias, el inventario y la clasificación automática de ellos mismos por tipologías, de sus datos relevantes (ubicación, sistema operativo, firmware, versión), sus vulnerabilidades a nivel de ciberseguridad, su posible grado de infección, y en general la detección y priorización de los riesgos de ciberseguridad, así como la posibilidad de tomar contramedidas de carácter preventivo o reactivo locales a los centros. Para ello será preciso un suministro y configuración inicial, unos servicios avanzados de configuración e integraciones y el diseño y prueba del sistema de monitorización y aseguramiento de la calidad. En resumen, el sistema a implantar debe conseguir los siguientes objetivos:

- Visibilidad, inventario, detección y clasificación de activos de forma constante. Es preciso monitorizar los equipos conectados en tiempo real.

- Gestión preventiva de riesgos:

- o Detección de vulnerabilidades. Es preciso conocer el nivel de seguridad y vulnerabilidades que afectan a los dispositivos, para mejorar la seguridad de forma continua.

- o Detección de amenazas y ataques.

- Capacidad de respuesta ante esos ataques que se produzcan, que puede realizarse de dos formas, no necesariamente alternativas:

- o Enriqueciendo los datos de los SIEM, para mejorar la observabilidad de la red

- o Mediante integraciones con un NAC y/o con los cortafuegos de cada edificio.

Por lo que respecta a los motivos de la tramitación urgente del expediente, queda reflejada en la propuesta de contratación la urgencia en la tramitación de este expediente es la finalidad de dotar a la red de comunicaciones de los Centros de Salud de Atención Primaria del Servicio Madrileño de Salud

Exp.: **A/SUM-045459/2024**

*Unidad administrativa:*  
**DIVISIÓN DE CONTRATACION**

de un mejor sistema de control y seguridad de los equipos conectados que redunde en impedir los ciberataques dirigidos al sector sanitario español, intentos que son cada vez más frecuentes. Se estima que su tramitación inmediata es de interés público por cuanto las consecuencias de los posibles ciberataques pueden provocar el cese total o parcial de su actividad, con las implicaciones que esto puede generar en la población.

La necesidad de esta tramitación se debe a que es un entorno con un número importante de dispositivos médicos de naturaleza heterogénea, y en el que se maneja información médica de los pacientes

De todo lo anterior se desprende que concurren las razones de intereses público previstas en el artículo 119 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.

Por lo tanto, y con el objeto de dar cumplimiento a los preceptos citados y con el fin de poder adjudicar este contrato mediante el procedimiento abierto, con multiplicidad de criterios, se hace necesaria la tramitación por urgencia del correspondiente expediente de contratación.

**EL CONSEJERO DE DIGITALIZACIÓN**

P.D. Orden 47/2024, de 1 de abril (BOCM 16/04/2024)

**EL VICECONSEJERO DE DIGITALIZACIÓN.**

Firmado digitalmente por: PÉREZ GÓMEZ MANUEL  
Fecha: 2024.12.11 13:38