

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.

MEMORIA JUSTIFICATIVA DE INSUFICIENCIA DE MEDIOS PARA EL EXPEDIENTE DE CONTRATACIÓN MIXTO DE SUMINISTRO Y SERVICIOS DE 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) .

A los efectos previstos en el artículo 116.4 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público se informa lo siguiente:

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.

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, en 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 (IoMT, 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.


A los efectos previstos en el artículo 116.4 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en el que se requiere la justificación de insuficiencia de medios, se informa lo siguiente:

Para satisfacer las necesidades anteriormente relacionadas, se pretende contratar un contrato mixto por contener prestaciones propias de suministro y servicios, y encontrarse ambas prestaciones directamente vinculadas entre sí manteniendo una relación de complementariedad que exige su consideración y tratamiento como una unidad funcional cuyo objeto es **CONTRATACIÓN MIXTO DE SUMINISTRO Y SERVICIOS DE 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.**

De cara a la correcta realización de estas tareas y dada la carencia de personal propio con la adecuada especialización en la evolución de los sistemas informacionales actuales, se considera necesario e imprescindible proceder a la contratación de los servicios requeridos, de acuerdo a las condiciones indicadas en la documentación del expediente de contratación.

Madrid,

LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: NURIA RUIZ HOMBREBUENO - 
Fecha: 2024.12.30 14:53