

INFORME DE INSUFICIENCIA DE MEDIOS

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.

CONSEJERÍA/ORGANISMO CONTRATANTE: Consejería de Digitalización

CÓDIGO EXPEDIENTE: A/SER-049688/2024

TIPO CONTRATO: Servicios

TÍTULO EXPEDIENTE: CONTRATACIÓN DEL DISEÑO, IMPLEMENTACIÓN, PUESTA EN MARCHA Y DINAMIZACIÓN DE UN CENTRO DEMOSTRADOR PARA EXPERIMENTACIÓN EN CIBERSEGURIDAD DEL SECTOR SALUD, EN EL ÁMBITO DEL PROGRAMA RETECH (Redes Territoriales de Especialización Tecnológica) Y EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA – NEXT GENERATION EU

OBJETO DEL CONTRATO: Identificación del estado de la ciberseguridad en el sector salud, creación de un conjunto de casos de uso para abordar los principales retos y problemas identificados, despliegue de un entorno tecnológico que permita reproducir los casos de uso de forma realista y definición y diseño de un catálogo de servicios que aporte valor a todas las partes involucradas en el sector salud, así como la dinamización del centro demostrador y sus servicios.

TIPO DE TRAMITACIÓN: Urgente

PROCEDIMIENTO DE CONTRATACIÓN: Abierto

TRAMITACIÓN ECONÓMICA: Ordinaria

JUSTIFICACIÓN DE LA NECESIDAD:

El 29 de mayo de 2024 se firmó el Convenio de colaboración en el ámbito de la convocatoria RETECH entre la Comunidad de Madrid y la S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A. (INCIBE). La firma de dicho Convenio tiene por objeto desarrollar y ejecutar el PROYECTO RESEDA, por la Comunidad de Madrid e INCIBE, alineándose así con la Agenda España Digital 2026 y contribuyendo a la consecución del Componente 15.17 del Plan de Recuperación, Transformación y Resiliencia, con la cual INCIBE, en tanto que Entidad de referencia para el desarrollo de la ciberseguridad, tiene interés en colaborar al formar parte de sus objetivos estratégicos tal consecución.

Dicho Convenio especifica que la entidad designada por la Comunidad de Madrid para la realización del PROYECTO RESEDA es la Consejería de Digitalización.

El PROYECTO RESEDA tiene como finalidad impulsar y fortalecer el ecosistema nacional de ciberseguridad, mediante la generación de capacidades especializadas en el ámbito de salud, buscando asegurar tanto la complementariedad, la colaboración público-privada, la participación de los agentes necesarios para constituir este ecosistema de innovación, la cohesión social y territorial, la generación de talento digital, la creación de empleo y emprendimiento, el posicionamiento internacional, como su viabilidad y sostenibilidad, y enfocado a mejorar la competitividad de las

empresas y de las Pymes en particular, alineándose así con el Eje 3 de la Agenda España Digital 2026 y contribuyendo a la consecución del Componente 15.17 del Plan de Recuperación, Transformación y Resiliencia.

La ciberseguridad aplicada al sector sanitario se ha convertido en una cuestión de la máxima relevancia. El proceso de transformación digital que está experimentando el sector hace que los servicios clínicos y hospitalarios dependan fuertemente de las infraestructuras digitales. La automatización está alcanzando no solo a los servicios de gestión del paciente y a otros servicios de soporte (logística, contabilidad y finanzas, compras, etc.) si no que afecta también a los equipos clínicos y de laboratorio. Los dispositivos médicos conectados están transformando la forma en que funciona el sector, tanto dentro de los hospitales como entre los diferentes actores de la industria de la salud.

Sin embargo, el aumento de los flujos de información dentro y fuera de los hospitales y las clínicas, conlleva riesgos importantes que necesitan ser abordados. Algunos de los riesgos comprenden daños a la seguridad del paciente o pérdida de información personal, que pueden ser causados por acciones maliciosas, por errores humanos, del sistema o de terceros, y por fenómenos naturales. A medida que la superficie de ataque aumenta con la introducción de nuevos dispositivos conectados, la probabilidad y el posible impacto de los ataques crece exponencialmente.

Las actividades de la Comunidad de Madrid se centrarán en impulsar una red de empresas e instituciones, públicas y privadas, que trabajen para reforzar la ciberseguridad en el sector salud, contribuyendo a que todos los centros y unidades, públicos y privados, refuercen la protección de los datos personales y la seguridad de los equipos, dispositivos médicos y los sistemas implantados. Para ello, impulsa el desarrollo de nuevos productos y servicios específicamente diseñados para su utilización en el entorno clínico-hospitalario, aumentando la oferta de soluciones y servicios de las empresas españolas.

Las actuaciones a realizar incluyen las siguientes líneas de actuación, relacionadas con el sector estratégico salud:

- Línea de actuación 1 – Identificación del estado de la ciberseguridad en los subsectores elegidos y creación de un conjunto de casos de uso (entre 15 y 20) para abordar los principales retos y problemas relacionados con la protección de la información, los servicios, los equipos y sistemas de Smart Health.
- Línea de actuación 2 – Despliegue de un entorno tecnológico que permita reproducir de la forma más realista y fiel posible, los casos diseñados en la línea de actuación anterior, y aporte las facilidades necesarias para explotar de forma presencial o remota los servicios que se van a ir desplegando en la línea de actuación 3.
- Línea de actuación 3 – Definición y diseño de un catálogo de servicios que aporte valor a todas las partes interesadas, organizaciones sanitarias públicas y privadas, empresas especializadas, emprendedores, profesionales y personas interesadas en adquirir conocimientos para entrar en el mercado profesional de la ciberseguridad.

Teniendo en cuenta la naturaleza del proyecto, estas tres líneas de actuación se complementan. Así, el desarrollo de “casos de uso” tiene por objeto identificar el tipo y naturaleza de las amenazas en el sector salud e identificar los escenarios y las soluciones y medidas de distinto tipo que deben desarrollarse. En el Centro Demostrador se harán análisis de simulación, test de soluciones, pruebas, etc., así como formación. Por último, partiendo de un catálogo o inventario inicial que recoja el estado del sector en materia de ciberseguridad, conforme se vayan incorporando los casos de uso y las diferentes soluciones, se irá completando un Catálogo que permitirá al final del periodo, ofrecer una visión de la oferta de soluciones y servicios para hacer frente a las amenazas y riesgos.

El objetivo global del proyecto es el impulso a la ciberseguridad en el sector salud, mejorando el posicionamiento y la especialización inteligente de las empresas, incentivando la innovación, la formación y la concienciación con soluciones.

Para lograr este objetivo se hace necesario llevar a cabo las tres líneas de actuación referenciadas anteriormente realizando además acciones de divulgación que permitan poner al centro demostrador en conocimiento de la ciudadanía, las empresas y de las instituciones y efectuando la transferencia del servicio de modo que se consiga la sostenibilidad y continuidad futura del centro demostrador. Estas actuaciones constituyen el objeto del contrato.

Este contrato está financiado por la Unión Europea a través del Mecanismo de Recuperación y Resiliencia-NextGeneration EU, del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España.

INSUFICIENCIA DE MEDIOS:

Es importante destacar que el diseño, implementación y puesta en marcha de un centro demostrador representativo del sector salud exige, por un lado, un nivel de conocimiento técnico altamente específico y especializado, que no está disponible dentro de la Dirección General de Estrategia Digital, que no cuenta con los perfiles específicos que se exigen en el presente contrato siendo necesario además un número de recursos humanos que supera los disponibles en dicha Dirección General; y, por otro lado, exige el disponer de los equipos necesarios que permitan desarrollar los casos de uso previamente analizados por el personal especializado. Dichos equipos tampoco están disponibles en la Dirección General de Estrategia Digital.


Es por ello que la única solución es recurrir a empresas especializadas que cuenten con la experiencia y el conocimiento necesarios para el despliegue de infraestructuras en entornos reales, así como con el número de medios humanos necesarios, con el perfil específico, exigidos en el presente contrato.

En virtud de lo dispuesto en los artículos 30.3 y 116.4. f) 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, se emite el presente informe, por el que se justifica la carencia de medios propios

suficientes en el órgano de contratación, para la prestación de los servicios objeto de licitación que figuran en el encabezamiento.

En Madrid, a fecha de la firma

El Director General de Estrategia Digital

Firmado digitalmente por: IGNACIO JULEN AZORIN GONZALEZ - 
Fecha: 2025.02.21 14:05