

Informe de Insuficiencia de Medios Propios para “**SERVICIO DE DESARROLLO, IMPLANTACIÓN Y EJECUCIÓN DE UN PROGRAMA DE FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD PARA PERSONAL SANITARIO Y DE LAS ENTIDADES LOCALES**”, a adjudicar mediante procedimiento abierto con pluralidad de criterios, bajo el marco del Proyecto RETECH, alineado con la Agenda España Digital 2026 y el Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea – NEXT GENERATION EU

Expediente: **ACR-037-2025**



INDICE:

1	INTRODUCCIÓN	3
1.1	Objeto del contrato.....	3
1.2	Finalidad del informe.....	3
2	FUNCIONES A CUBRIR MEDIANTE EL CONTRATO.....	3
3	MEDIOS PERSONALES Y TÉCNICOS DISPONIBLES EN LA AGENCIA	4
3.1	Recursos personales	4
3.2	Recursos técnicos y organizativos	4
4	JUSTIFICACIÓN DE LA INSUFICIENCIA O INADECUACIÓN DE MEDIOS PROPIOS	5
5	CONCLUSIÓN	5

1 INTRODUCCIÓN

1.1 Objeto del contrato

El objeto del presente contrato es la prestación de un servicio integral para el diseño, ejecución, dinamización y evaluación de un programa global de formación práctica y de sensibilización en ciberseguridad, dirigido al personal del sector sanitario y de las entidades locales de la Comunidad de Madrid, en el marco de la iniciativa RESEDA.

El servicio comprenderá la planificación, preparación técnica, ejecución y evaluación de un conjunto de actividades, distribuidas en distintas tipologías, que incluyen:

- **Hackathones** orientados al aprendizaje colaborativo mediante retos sectoriales de innovación.
- **Ciberejercicios**, centrados en la simulación de incidentes reales y el entrenamiento operativo de respuesta.
- **Sesiones de formación dirigidas a perfiles de alta dirección**, con enfoque estratégico y de gobernanza.
- **Campañas de sensibilización frente a phishing** (incluyendo modalidades de smishing y vishing), orientadas a reforzar las capacidades de detección y respuesta del personal sanitario y del personal de las entidades locales frente a intentos de ingeniería social.
- **Sesiones temáticas especializadas**, centradas en ámbitos tecnológicos emergentes y casos prácticos de aplicación en el entorno sanitario y local.

Con esta contratación se persigue alcanzar los siguientes objetivos estratégicos:

1. Mejorar las competencias en ciberseguridad mediante actividades formativas estructuradas, dinámicas prácticas y métricas de aprovechamiento.
2. Desarrollar cultura de ciberseguridad mediante la implicación activa de los profesionales en ejercicios colaborativos y campañas de sensibilización frente a ingeniería social.
3. Sensibilizar a los órganos de dirección sobre los riesgos, decisiones y responsabilidades en materia de ciberseguridad, mediante sesiones específicas adaptadas a su rol estratégico.
4. Promover el conocimiento aplicado en ámbitos tecnológicos emergentes, con sesiones especializadas que permitan trasladar a la práctica conceptos avanzados de seguridad.
5. Evaluar el impacto del programa de forma estructurada, mediante indicadores clave de rendimiento (KPIs), informes técnicos e instrumentos de análisis comparativo que faciliten la mejora continua de las acciones de capacitación y sensibilización.

1.2 Finalidad del informe

Este informe tiene como finalidad dejar constancia de la insuficiencia de medios personales y técnicos propios en la Agencia de Ciberseguridad de la Comunidad de Madrid para ejecutar internamente las tareas especializadas descritas en el objeto del contrato. Se emite conforme a lo previsto en el artículo 116.4 de la Ley 9/2017, de Contratos del Sector Público, con el fin de justificar la necesidad de recurrir a una contratación externa.

2 FUNCIONES A CUBRIR MEDIANTE EL CONTRATO

El contrato tiene por finalidad proporcionar a la Agencia de Ciberseguridad de la Comunidad de Madrid un servicio integral de formación práctica y sensibilización en ciberseguridad, dirigido al personal del sector sanitario y de las entidades locales, en el marco de la iniciativa RESEDA.

Su objetivo es diseñar, ejecutar y evaluar un conjunto coordinado de acciones formativas, ejercicios técnicos y campañas de concienciación, orientadas a reforzar las capacidades institucionales frente a las amenazas cibernéticas y a promover una cultura de seguridad sostenida en el tiempo.

Entre las funciones específicas incluidas en el contrato destacan:

- Diseño pedagógico y técnico del programa global de formación y sensibilización, incluyendo la definición de metodologías, itinerarios y formatos de aprendizaje adaptados a distintos perfiles profesionales.
- Planificación, organización y ejecución de hackathones y ciberejercicios, concebidos como actividades prácticas de entrenamiento ante incidentes reales o simulados.
- Desarrollo de materiales técnicos y didácticos, guías, recursos audiovisuales y contenidos digitales accesibles, orientados tanto a la formación presencial como virtual.
- Diseño y ejecución de campañas de sensibilización frente a ataques de ingeniería social, incluyendo simulaciones de phishing, smishing y vishing, con métricas de impacto y aprendizaje.
- Realización de sesiones específicas para alta dirección, centradas en la gestión estratégica del riesgo, la gobernanza de la ciberseguridad y la toma de decisiones ante incidentes.
- Diseño y dinamización de sesiones temáticas especializadas, enfocadas en tecnologías emergentes, ciberamenazas actuales y buenas prácticas aplicadas al entorno sanitario y local.
- Elaboración de indicadores de rendimiento (KPIs), informes técnicos y análisis comparativos, que permitan medir el grado de aprovechamiento, eficacia y transferencia de conocimiento.
- Apoyo técnico y metodológico a la Agencia durante la supervisión y evaluación del programa, garantizando la coherencia con los estándares del ENS, la Directiva NIS2 y el marco estratégico regional de ciberseguridad.

Estas tareas requieren alta especialización técnica, experiencia en formación avanzada en ciberseguridad y conocimiento de entornos institucionales complejos, así como capacidad para desplegar entornos de simulación y metodologías activas de aprendizaje en contextos reales de prestación de servicios públicos.

3 MEDIOS PERSONALES Y TÉCNICOS DISPONIBLES EN LA AGENCIA

3.1 Recursos personales

La Agencia de Ciberseguridad no dispone en la actualidad de personal técnico especializado en formación práctica avanzada en ciberseguridad, diseño de ciberejercicios o campañas de sensibilización a gran escala.

El personal existente desarrolla funciones de coordinación, supervisión y apoyo metodológico, pero no cuenta con dedicación específica ni con experiencia acreditada en la planificación, dinamización y evaluación de programas formativos complejos de este alcance y naturaleza técnica.

Asimismo, la estructura actual de la Agencia no incluye unidades con capacidad operativa para el desarrollo directo de hackathones, ciberejercicios o simulaciones de incidentes, ni personal dedicado a la gestión de plataformas de simulación o entornos de entrenamiento.

3.2 Recursos técnicos y organizativos

No se dispone de infraestructura técnica, herramientas de simulación, ni plataformas de formación y seguimiento que permitan desarrollar internamente las actividades contempladas en el contrato. La Agencia no cuenta con entornos virtualizados o cyber-ranges para ejercicios técnicos, ni con recursos tecnológicos para la gestión integral de campañas de phishing o programas de concienciación masiva.

4 JUSTIFICACIÓN DE LA INSUFICIENCIA O INADECUACIÓN DE MEDIOS PROPIOS

La ejecución de un programa integral de formación práctica y sensibilización en ciberseguridad como el previsto requiere:

- Conocimiento experto en diseño pedagógico y técnico de programas avanzados de ciberseguridad, incluyendo la planificación y dinamización de ejercicios prácticos.
- Experiencia acreditada en la organización de hackathones, ciberejercicios y campañas de sensibilización en entornos institucionales o sectoriales.
- Capacidad para desarrollar y operar plataformas técnicas de simulación, registro y análisis de resultados, así como herramientas de seguimiento y evaluación de impacto.
- Competencia metodológica en la medición de indicadores de desempeño y elaboración de informes de resultados aplicables a acciones formativas especializadas.
- Conocimiento actualizado de los marcos normativos ENS, NIS2 y estrategias de ciberseguridad institucional, para garantizar la coherencia del programa con las políticas públicas vigentes.

Estas capacidades no están disponibles actualmente en el personal ni en la estructura técnica de la Agencia de Ciberseguridad de la Comunidad de Madrid, ni pueden desarrollarse internamente en los plazos requeridos por la planificación del proyecto.

Tampoco se dispone de un equipo especializado que pueda asumir la ejecución directa de las actividades sin un esfuerzo desproporcionado o sin comprometer otras funciones esenciales de la Agencia.

Dado que el contrato debe desarrollarse en un periodo limitado y con resultados verificables, y que exige una alta especialización técnica y metodológica, resulta inviable abordar su cumplimiento con medios propios, siendo necesario recurrir a la contratación externa para garantizar la eficacia, calidad y oportunidad de los resultados esperados.

5 CONCLUSIÓN

A la vista de lo expuesto, se concluye que la Agencia de Ciberseguridad de la Comunidad de Madrid **no dispone de los medios personales ni técnicos suficientes para ejecutar con recursos propios** las tareas objeto del contrato.

La correcta ejecución del contrato requiere conocimientos especializados, experiencia operativa, capacidad metodológica y disponibilidad inmediata de recursos técnicos y humanos. Estos elementos no se encuentran actualmente disponibles en la estructura interna de la Agencia. En consecuencia, se justifica plenamente la necesidad de recurrir a la contratación externa para garantizar la calidad, eficacia y oportunidad de las actuaciones previstas, así como para reforzar las capacidades institucionales y la cultura de ciberseguridad en el ámbito sanitario y local de la Comunidad de Madrid.