# Informe sobre la Consulta Preliminar de Mercado sobre Laboratorio Especializado para la Evaluación y Mejora de la Ciberseguridad de Productos IoT e IA para los Sectores de la Salud y las Smart Cities



Dirección General de Estrategia Digital
T: 955061501
dged.ada@juntadeandalucia.es

# 1. Introducción

La Agencia Digital de Andalucía, en la línea de homogeneización y simplificación que subyace en las competencias sobre ciberseguridad, se plantea el establecimiento de un laboratorio especializado para la evaluación y mejora de la Ciberseguridad de los productos IoT e IA para los sectores de la Salud y las Smart Cities

Con el fin de recabar información de los operadores económicos relativa al objeto de dicha contratación y para ayudar en la posible elaboración futura de los pliegos correspondientes a un expediente de contratación, se abrió con fecha 12 de abril de 2024 una consulta preliminar de mercado, que puede ser accedida en la siguiente dirección:

https://www.juntadeandalucia.es/haciendayadministracionpublica/apl/pdc_sirec/perfiles-licitaciones/consultas-preliminares/detalle.jsf?idExpediente=128

Este documento constituye el informe contemplado en el artículo 115.3 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.

# 2. Consulta y respuestas recibidas

La consulta exponía la situación actual de competencias en materia de ciberseguridad a raíz del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (en adelante ADA).

Estas competencias, en virtud del artículo 15.3.c de los Estatutos, serán desarrolladas por la Dirección General de Estrategia Digital y su principal marco de desarrollo es la Estrategia de Ciberseguridad de Andalucía 2022 – 2025, que tiene entre sus líneas de actuación

- El fortalecimiento y desarrollo de marcos de cooperación y colaboración en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional (Línea de Actuación 3).
- El desarrollo de programas para el impulso y financiación de la ciberseguridad en el sector empresarial andaluz, favoreciendo la mejora de su nivel de madurez (Línea de Actuación 4).
- El establecimiento de planes de desarrollo de una industria especializada en el sector de la ciberseguridad a lo largo del territorio andaluz (Línea de Actuación 5).
- La creación y el desarrollo de un plan de promoción de Andalucía, posicionándola como territorio de referencia en materia de ciberseguridad (Línea de Actuación 6).
- La elaboración y el despliegue de programas formativos con contenidos de ciberseguridad, así como de planes de formación continua y reciclaje para profesionales del sector (Línea de Actuación 7).

La participación de la Comunidad Autónoma de Andalucía, a través de la Agencia Digital de Andalucía, en el proyecto Red Argos, dentro del marco del programa RETECH, se ajusta a estas líneas, estableciendo un

marco de colaboración con INCIBE y con las Comunidades Autónomas de Castilla-León y País Vasco en el que se establecen programas de especialización inteligente para cada una de ellas en ámbitos específicos de la Ciberseguridad.

Los ámbitos que asume Andalucía son los de la Salud y las Smart Cities. Asumiendo un enfoque basado en el estado actual de la tecnología y sus principales líneas de evolución futura, serán objeto de especial atención la Inteligencia Artificial (en adelante, IA) y la Internet de las cosas (en adelante, IoT).

Se solicitaba de los participantes la remisión de un cuestionario con:

I. Observaciones sobre el alcance y las componentes del laboratorio.

II. Necesidades de instalaciones e infraestructura.

III. Normativa y marcos de aplicación.

IV. Necesidades de equipamiento y materiales.

V. Necesidades de personal.

VI. Otra información que sea considerada como relevante por la entidad que rellena el formulario.

VII. Estimación económica para los distintos elementos involucrados.

Dada la amplitud y diversidad de las actividades que pueden abordarse en el ámbito de este laboratorio (análisis, propuestas de mejora, certificación, en ámbitos de IA y de IoT...), en el texto de la consulta preliminar de mercado se indicó de forma expresa que se admitirían respuestas parciales que abordaran el campo de experiencia de las entidades participantes.

Se estableció inicialmente el día 21 de abril de 2024 como fecha límite para remitir los cuestionarios cumplimentados a través de la Presentación Electrónica General de la Junta de Andalucía, con destino a la Dirección General de Estrategia Digital de la Agencia Digital de Andalucía. Posteriormente, ante las solicitudes de varias entidades interesadas en responder a la consulta que manifestaron sus dificultades para entregar una información completa en ese plazo, se acordó la ampliación del mismo hasta el día 30 de abril de 2024.

A la finalización del plazo de remisión, se habían recibido respuestas formales de nueve (9) entidades que remitieron el cuestionario relleno:

- D.med Software.
- DEKRA Testing and Certification, S.A.U.
- Telefónica Soluciones de Informática y Comunicaciones de España S. A.
- Fundación Instituto Ricardo Valle de Innovación (INNOVA IRV), a través de su unidad conjunta de innovación EURECAT-INNOVA IRV.
- Fujitsu Technology Solutions S.A.U.
- IaaS365.
- JTSEC BEYOND IT SECURITY SLU.
- INNOVA IRV Microelectronics S.L.
- Tecnologías Plexus S.L.

# 3. Conclusiones

Recibidos los cuestionarios, se comenzó el análisis de la información suministrada. Del análisis realizado por el Servicio de Ciberseguridad de la Dirección General de Estrategia Digital cabe extraer las siguientes conclusiones:

## 3.1. Alcance y componentes

### 3.1.1. Unidades del laboratorio

Una de las respuestas apuntó al uso de cuatro productos como unidades de evaluación:

- TXone Edge IPS: Dispositivo de protección de entornos OT
- StellarOne: Protección endpoint para entornos OT
- Portable Security 3: dispositivo USB sin instalación para análisis de malware
- Trend Micro Mobile Security: Protección para entornos 5G

Otra se centraba exclusivamente en la composición de un laboratorio 5G.

Otra definía dos sublaboratorios, uno para Smart Cities y otro para Salud, indicando tipos de dispositivos a probar en cada uno de ellos. Después, establecía unas componentes comunes tras ellos: computación Edge, Cloud, Máquinas virtuales, Datos e IA.

La siguiente lista indica las componentes mencionadas en el resto de las respuestas, así como en la mencionada en el párrafo anterior y el número de ellas en las que aparecieron. Nótese que las respuestas de cada subapartado no han sido computadas para el apartado superior salvo que se indicara de forma expresa en la respuesta:

- Electrónica / Hardware — 5 respuesta
  - Componentes hardware — 1 respuesta
    - Chips y componentes electrónicos — 1 respuesta
  - Interfaces hardware — 1 respuesta
  - Dispositivos (cámaras, móviles, sensores…) — 3 respuesta
  - Productos completos integrados — 1 respuesta
  - Sensores — 2 respuesta
- Comunicaciones — 2 respuesta

- Interfaces inalámbricas 1 respuesta
  - 5G 1 respuesta
  - Wifi 1 respuesta
  - Otras respuesta
- Cloud 2 respuesta

- Software 6 respuesta
  - Inteligencia Artificial 4 respuesta
  - Aplicaciones móviles 2 respuesta
  - Herramientas de evaluación/pentesting 1 respuesta
  - Herramientas de seguridad/protección 1 respuesta
- Servicios asociados 1 respuesta

  (gestión de datos, interoprerabilidad, gestión de identidades…)
- Certificación 1 respuesta
- Consultoría y formación y desarrollo 2 respuestas
- Desarrollo e integración de herramientas 1 respuesta
- Calidad y cumplimiento normativo 2 respuesta

Unidades menos importantes, al menos en un momento inicial, aunque, en algunos casos, posteriormente podrían cobrar relevancia

- Comunicaciones 1 respuesta
  - 5G 1 respuesta
- Servicios asociados 1 respuesta
- Desarrollo e integración de herramientas 1 respuesta
- Consultoría y formación y desarrollo 1 respuesta
- Cumplimiento normativo 1 respuesta

En cuanto a la demanda de cada módulo se tuvo

- Para empresas de ciberseguridad

- Con potencial mayor demanda:
  - Software 3 respuestas
  - IA 2 respuesta
  - Data lake 1 respuesta
  - Componentes hardware 2 respuesta
    - Productos completos integrados 1 respuesta
    - Dispositivos 2 respuesta
  - Interfaces hardware 1 respuesta
  - Herramientas de seguridad/protección 1 respuesta

- Con potencial menor demanda:
  - Comunicaciones 1 respuesta
    - 5G 1 respuesta
  - Desarrollo e integración de herramientas 1 respuesta
  - Consultoría y formación 1 respuesta
  - Calidad y cumplimiento normativo 2 respuesta
  - Servicios asociados 1 respuesta

- Para el resto de las empresas
  - Con potencial mayor demanda:
    - Software 1 respuesta
      - IA 4 respuestas
    - Componentes hardware 1 respuesta
    - Interfaces inalámbricas 1 respuesta
    - Hardware 1 respuesta
      - Chips y componentes 1 respuesta
      - Productos completos integrados 1 respuesta
      - Dispositivos 2 respuesta
    - Cumplimiento normativo 1 respuesta

- Con potencial menor demanda:
  - Comunicaciones 1 respuesta
    - 5G 1 respuesta
  - Data lake 1 respuestas
  - Servicios asociados 1 respuesta
  - Herramientas de seguridad/protección 1 respuesta

En una respuesta se planteó la oportunidad de crear sinergias con proyectos relacionados con la evaluación de chips y componentes electrónicos, como el nuevo centro de I+D de IMEC que se instalará en Málaga o el proyecto Dkulpiot.

Otra manifestó que, ante la problemática existente, la normativa existente en la actualidad o las dificultades para evaluar componentes, sería recomendable centrar el laboratorio en las componentes finales, algo que hacen ya algunos laboratorios existentes.

### 3.1.2. Tipos de actividades

Se plantearon supuestos de combinación de actividades en el laboratorio.

En particular, se indicó que una misma entidad podría actuar como certificadora como laboratorio, siempre que ambas unidades se encuentren debidamente separadas para garantizar su independencia.

### 3.1.3. Unidad para evaluación de 5G

De las respuestas recibidas:

- 1 se centra exclusivamente en un laboratorio 5G.
- 2 contempla una unidad de interfaces inalámbricas o redes que incluye, entre otras, las de 5G.
- 1 habla de comunicaciones en general, sin mencionar expresamente 5G.
- 1 establece la componente de evaluación/protección para entornos 5G como opcional.
- 1 indica que, pese a su importancia crítica en la comunicación entre dispositivos y con los servicios relacionados, el laboratorio 5G no resulta fundamental como elemento auxiliar para el sector de la ciberseguridad. Añade que podría sustituirse por un uso limitado de red wifi, pero que se debe tener en cuenta que existen pocos elementos IoT que permitan conexión wifi dado su alto consumo de batería.
- 3 no mencionan las comunicaciones en su respuesta.

## 3.2. Instalaciones e infraestructuras

En general, se señaló que no es necesario contar con grandes espacios para el laboratorio, si bien sus dimensiones dependerán de las unidades que se desplieguen y del alcance que se les quiera dar.

Cuatro de las respuestas dieron cifras aproximadas comprendidas en el rango 150-350 $m^2$.

Otras dos, en el rango 400-600 $m^2$.

Por lo general, en estas cifras no se incluyen zonas comunes como pasillos, almacenes, etc.

Se indicó que es conveniente mantener espacios separados para todas o, al menos, varias de las unidades. En particular, es importante el control de acceso y la protección contra intrusiones físicas, así como sistemas anti-incendios y otros que garanticen las condiciones ambientales óptimas para el funcionamiento del equipamiento.

A este respecto, por lo general, no se establecieron requisitos especiales que pudieran salirse de las condiciones ambientales normales. Sin embargo, se mencionó de forma expresa:

- Suministro estable de electricidad, con sistemas de alimentación ininterrumpida y protecciones contra sobretensiones. En varias respuestas se hizo referencia a la necesidad de contar con puntos de carga para los dispositivos.
- Una adecuada refrigeración.
- Una adecuada calidad del aire.
- Aislamiento de sonidos.
- Correcta iluminación.
- Protección contra interferencias electromagnéticas.

Esto conlleva la existencia de elementos que sirvan tanto para mantener esas condiciones en unos márgenes aceptables como medir y registrar sus valores.

También se señaló la necesidad de contar con otros suministros y servicios como:

- Aire comprimido, en especial, en lo relacionado con los dispositivos médicos.
- Agua, también especialmente en lo relacionado con dispositivos médicos y la refrigeración de equipos. En algún caso, al tratar sobre Smart Cities, la respuesta indicó de forma expresa que para ese ámbito no sería necesario.
- Gestión de residuos.
- Limpieza.
- Copias de respaldo de la información.

En cuanto a los requisitos de comunicaciones, se indica, en general, la necesidad de una red que garantice la conectividad entre los elementos del laboratorio, así como con recursos externos y sistemas de prueba en la nube. Esta infraestructura deberá permitir la creación y gestión de diferentes segmentos de red, así como su aislamiento o conectividad según se necesite, al igual que con la conexión hacia el exterior (Internet). En todo caso, se señaló que el acceso a una red pública por parte de los elementos debería ser un caso excepcional y debidamente justificado.

También se menciona la existencia de una red para el personal del laboratorio que permita la comunicación y colaboración de forma segura.

## 3.3. Normativa y marcos

En la consulta se planteaba la posibilidad de exigir certificaciones en ISO 17025, "Requisitos generales para la competencia de los laboratorios de ensayo y calibración", e ISO 17065, "Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios" a las empresas involucradas en la gestión y operación del laboratorio y se preguntaba acerca de la existencia de otras normas y estándares aplicables o que pudieran reemplazarlos.

Las respuestas indicaron que:

- En 1 caso, que los laboratorios de ciberseguridad suelen estar acreditados por ENAC en la ISO/IEC 17025.
- En 2 casos se indicó la conveniencia o coherencia de requerir ISO 17025.
- En 1 caso, la acreditación ISO 17025 se condicionó a la realización de ensayos y la emisión de informes.
- En 1 caso, la acreditación ISO 17025 se condicionó a que los informes del laboratorio fueran vinculantes para obtener una certificación.
- En 1 caso se indicó que la certificación ISO 17025 podría ser valorable, pero no debería ser exigible.
- En 1 caso se indicó la conveniencia o coherencia de requerir ISO 17065.
- En 1 caso se indicó que la certificación ISO 17065 podría ser valorable, pero no debería ser exigible.
- En 1 caso se señaló que ISO 17065 solo debería ser exigible si el laboratorio exigiera certificaciones.
- En 1 caso se mencionó como posible requisito ISO 27001
- Em 1 caso se mencionó la conveniencia de la familia ISO 27xxx.
- En 1 caso se mencionó como posible requisito NIST Cybersecurity Framework
- En 1 caso se mencionó ISO 62443 en relación con el sector salud (requerimientos y pentesting).
- En 1 caso se mencionó ISO 81001-5-1 en relación con el sector salud (pautas de desarrollo y documentación).
- En 1 caso se mencionó como posible requisito ISO 22301.
- En 2 casos se mencionó como posible requisito ENS, en uno de los cuales se hizo referencia al nivel Alto.
- En 1 caso se mencionó la posible consideración de ISO 31000 para la gestión de riesgos.

Por el contrario:

- En 1 caso se indicó que no se consideraba necesario ISO 17025, por estar más relacionada con otros tipos de laboratorio (biológico, químico, etc.).

- En 1 caso se indicó que no se consideraba necesario ISO 17065, más relacionada con certificaciones de productos y procesos.
- En 1 caso se planteó el uso de esquemas de certificación privados como alternativa a ISO 17065.
- En 1 caso se contempló la posibilidad de sustituir el requisito de ISO 17025 e ISO 17065 por ISO 27001 e ISO 27701 más el posible cumplimiento de ISO 27002 e ISO 27031.

También se hizo referencia a la necesidad de contemplar la siguiente normativa:

- Cyber Resilience Act (Smart Cities)
- MDR/IVDR (Salud)
- NIS2 (Smart Cities y Salud, para entidades esenciales e importantes)
- Digital Act & Data Act (Smart Cities y Salud))
- AI Act (Smart Cities y Salud)
- AI Liability Act (Smart Cities y Salud)
- Cyber Resilience Act (Smart Cities)
- European Chip Act (Smart Cities y Salud)

Además se hizo referencia a los siguientes marcos y estándares:

- Productos y componentes Hardware (dispositivos)
    - EN 18031-1 y EN 18031-2 (en desarrollo) (Smart Cities, productos con conectividad radio)
    - ETSI EN 303 645 (Smart Cities, seguridad de producto con nivel de seguridad básico)
    - IEC 62443-4-1 (Smart Cities, desarrollo de producto)
    - IEC 62443-4-2 (Smart Cities, seguridad de producto con nivel de seguridad substancial)
    - ISO 15408 / Common Criteria (Smart Cities, desarrollo y seguridad de producto con nivel de seguridad alto)
    - IEC 81001-5-1 (Salud, desarrollo de producto)
    - IEC 60601-4-5 (Salud, seguridad de producto)
    - OWASP Internet of Things (dispositivos IoT)
    - Connectivity Standards Alliance (CSA) IoT Device Security Specification (dispositivos IoT)
    - ISO 13485: requisitos para un sistema de gestión de la calidad en la fabricación de dispositivos médicos.

- ISO 14971: directrices para la gestión de riesgos asociados con los dispositivos médicos.
- ISO 14971: gestión de riesgos en el contexto de los productos médicos integrados.

- Productos y componentes Software (aplicaciones y cloud)
  - IEC 62443-4-1 (Smart Cities, desarrollo de producto)
  - IEC 62443-4-2 (Smart Cities, seguridad de producto con nivel de seguridad substancial)
  - ISO 15408 / Common Criteria (Smart Cities, desarrollo y seguridad de producto con nivel de seguridad alto)
  - ANSI UL 2900-2-1 (Salud, seguridad de producto) (Nota: este estándar está siendo reemplazado por lo que se citan a continuación)
  - IEC 81001-5-1 (Salud, desarrollo de producto)
  - IEC 60601-4-5 (Salud, seguridad de producto) . En 2 ocasiones.
  - OWASP MASVS (aplicaciones móviles)
  - OWASP Top 10 (aplicaciones cloud)
  - Connectivity Standards Alliance (CSA) IoT Device Security Specification (productos IoT)
- Productos y componentes Software (aplicaciones y cloud)
  - IEC 62443-4-1 (Smart Cities, desarrollo de producto)
  - IEC 62443-4-2 (Smart Cities, seguridad de producto con nivel de seguridad substancial)
  - ISO 15408 / Common Criteria (Smart Cities, desarrollo y seguridad de producto con nivel de seguridad alto)
  - ANSI UL 2900-2-1 (Salud, seguridad de producto) (Nota: este estándar está siendo reemplazado por lo que se citan a continuación)
  - IEC 81001-5-1 (Salud, desarrollo de producto)
  - IEC 60601-4-5 (Salud, seguridad de producto)
  - OWASP MASVS (aplicaciones móviles)
  - OWASP Top 10 (aplicaciones cloud)
  - Connectivity Standards Alliance (CSA) IoT Device Security Specification (productos IoT)
  - IEC 62304: requisitos para el ciclo de vida del software en dispositivos médicos.
- Productos y componentes de Inteligencia Artificial (IA)
  - ISO/IEC 27090 (en desarrollo) (Smart Cities y Salud)
  - ISO 24029 (Smart Cities y Salud)

  - ISO/IEC 5259 (en desarrollo) (Smart Cities y Salud)
  - ISO 42001 (Smart Cities y Salud, para sistemas de gestión)
  - ISO/IEC 27018: directrices para la protección de la información de salud personal (PHI) en la nube.
- Evaluación de chips y componentes electrónicos
  - PSA (Smart Cities, seguridad de producto con nivel de seguridad básico)
  - SESIP (Smart Cities, desarrollo y seguridad de producto con nivel de seguridad substancial)
  - ISO 15408 / Common Criteria (Smart Cities, desarrollo y seguridad de producto con nivel de seguridad alto)
- GDPR (RGPD)
- EIDAS
- Código de Derecho de la Ciberseguridad.
- EU IA Act
- CEN-CENELEC JTC 21
- Directiva RED.

## 3.4. Equipamiento y otras necesidades específicas

Si bien el software dependerá de las unidades a desplegar en el laboratorio y su alcance, se señaló la necesidad de contar con software para:

- Gestión de máquinas virtuales donde desplegar sistemas, aplicaciones y herramientas.
- Herramientas para la simulación de redes.
- Servidores y equipos con distintos sistemas operativos.
- Almacenamiento, incluyendo sistemas de bases de datos.
- IA
- Software para evaluar la seguridad
  - Kali Linux
  - Parrot Security OS
  - Otras herramientas para pentesting, auditorías, ingeniería inversa, análisis forense, etc.
  - Análisis estático y dinámico de código.

- Simulación de condiciones de estress, fuzzing, etc.

- Software para análisis de malware
- Sistemas para gestión de incidentes.
- Herramientas de cifrado y protección de datos.
- Software para IA: Aprendizaje automático, entrenamiento, pruebas de muestras adversarias, etc.
- Software para diseño y/o simulación de circuitos.
- Software para análisis de señales.
- Entornos para desarrollo y gestión de versiones.
- Plataformas para gestión de servicios en la nube.

Será necesario contar con herramientas tanto open source como propietarias. Estas últimas pueden ser requeridas para evaluar determinados productos.

En cuanto al hardware, aunque también dependerá de las características del laboratorio, se mencionaron:

- Equipos servidores, tanto de propósito general como de virtualización.
- Electrónica de red: switches, routers, etc.
- Firewalls.
- Dispositivos de captura de tráfico
- Equipos para pruebas específicas y diagnóstico: dispositivos de radiofrecuencia, captura de señales en buses y otras interfaces, hardware de seguridad física, osciloscopios, herramientas de soldadura…
- Dispositivos para evaluar. Fueron mencionados en uno de los casos. Si bien estos dispositivos son, a priori, elementos que quizá no formen parte del laboratorio en sí, quizá sea conveniente contar con algunos para demostraciones.
- Equipamiento y antenas para 5G.
- Servidor rack para el despliegue organizado del equipamiento.
- Herramientas hardware para realización de ataques, tanto intrusivos como no intrusivos.
- Material para lectura y programación de componentes hardware.
- Material para modificar componentes hardware.
- Equipamiento para ataque a redes inalámbricas, teniendo en cuenta los protocolos usados por los dispositivos a evaluar.
- Hardware para la IA, como tarjetas GPU aceleradoras NVidia (H100, A100, A30, L4).

- Otros servidores de alto rendimiento.

En cuanto a material fungible, se mencionó la necesidad de contemplar:

- Cables y conectores.
- Baterías o pilas y elementos de carga para dispositivos IoT.
- Material de soldadura.
- Tarjetas SIM para pruebas de acceso a equipamiento móvil.
- Dispositivos de almacenamiento de información.
- Puntas de prueba, fusibles, resistencias, condensadores, componentes electrónicos, etc.

Finalmente, se indicaron algunas necesidades de mantenimiento periódico de equipamiento, manteniendo actualizadas, verificadas y calibradas las herramientas hardware y haciendo frente a las necesidades de licenciamiento del equipamiento usado.

Asimismo, hubo una recomendación de revisar anualmente el estado del laboratorio y estudiar posibles necesidades de ampliación y/o mejora.

## 3.5. Personal

Se señaló la necesidad de mantener una formación del personal que les permita mantener actualizados sus conocimientos y capacidades.

Con respecto al personal necesario para las distintas fases del proyecto, en algunas respuestas se estableció un mismo equipo para la puesta en marcha del laboratorio y su posterior gestión, explotación y mantenimiento.

En general, se señaló lo siguiente:

- Fases previas a la puesta en marcha del laboratorio (instalación, pruebas, etc.). Las respuestas oscilaron entre las 3 y las 12 personas, con valores que entraron en la mayor parte de los casos en el rango de 8 a 12.
    - Los roles incluyeron:
        - Gestión de Proyectos / Responsable de laboratorio
        - Documentación
        - Formación
        - Calidad y cumplimiento
        - Ingenieros/administradores de ciberseguridad, redes y sistemas

- Técnicos de instalaciones
- Asuntos generales: personal, compras, asistencia TIC, etc.

- En cuanto a su formación, en un caso se mencionó únicamente que la tuvieran en ciberseguridad. En otro se recomendó contar con titulaciones universitarias en las áreas de Informática, Electrónica y/o Telecomunicaciones, así como certificaciones o experiencia mínima de 3 años en puesto similar, según puesto. En otro, se señaló la conveniencia de contar con perfiles con grado de Doctor (Nivel MECES 4) y Máster (Nivel MECES 3) si el laboratorio va a desarrollar tareas de investigación o I+D+i y que para las labores de jefatura y dirección de proyectos los perfiles deben ser de Grado o Máster (MECES 2 y 3), y para las actividades de operación pueden considerarse perfiles de ciclos formativos de técnico superior y grado (MECES 1 y 2).

En cuanto a la gestión del laboratorio (por ejemplo, asignación de los recursos disponibles a las distintas entidades/unidades usuarias) y su explotación (por ejemplo, personal técnico para el manejo del equipamiento), se señalaron las siguientes necesidades:

- Número de efectivos: El número de personas osciló entre 5 y 25, estando los valores más comunes comprendidos en el rango entre 9 y 15.
- Los roles mencionados fueron:
  - Responsable de laboratorio / Gestión de proyectos.
  - Responsables de unidad
  - Analista/auditor de seguridad
  - Administradores de redes y sistemas
  - Especialistas en testeo de dispositivos IoT
  - Consultoría y Formación
  - Calidad y Cumplimiento
  - Desarrollo e integración de herramientas
  - Respuesta a incidentes
- Formación: en un caso se indicó que este personal debe tener perfil de ingeniería en ciberseguridad con certificaciones en la materia. Otra recomendó la posesión de tieulaciones universitarias en las áreas de Informática, Electrónica y Comunicaciones, complementadas con formación específica del área de trabajo y certificaciones en materia de seguridad o IA, según el caso. Para los puestos de soporte estos requisitos serían únicamente puntos valorables. Finalmente, otra respuesta recomendó un grado en Administración de Empresas para la persona responsable de la gerencia del laboratorio, mientras que para los gestores de proyectos indicaba formación técnica con experiencia en gestión de proyectos y para los puestos técnicos requería titulaciones universitarias o de FP afines a las funciones a realizar, así como conocimientos

específicos y, para los puestos de especialista en ciberseguridad, certificaciones en seguridad ofensiva.

El mantenimiento del equipamiento del laboratorio requeriría, según las respuestas obtenidas:

- Número de personas: Las respuestas oscilaron entre 2 y 9 personas, estando los valores más comunes comprendidos en el rango entre 3 y 5.
- Roles:
  - Soporte/administración de IT y sistemas.
  - Soporte/administración de redes.
  - Técnicos de hardware.
  - Técnicos de instalaciones.
  - Gestión de proveedores
- Titulaciones: En general, no se indicó ninguna. En un caso se mencionó la necesidad que los técnicos de soporte y administración de IT, sistemas y redes contaran con ingeniería infromática, FP ASIX o similar

Además de lo anterior, se señaló la necesidad de contar con perfiles de difusión y comunicaciones para diseminar las actividades realizadas en el laboratorio. Asimismo, se planteó la necesidad de contar con un equipo de gestión de cuentas y marketing compuesto por una jefatura y 3 gestores.

## 3.6. Otra información recogida

El número de elementos que se podrá probar en cada unidad de forma simultánea dependerá del tamaño del laboratorio, así como de la complejidad de cada prueba. Algunas aproximaciones mencionaron que:

- Podría estar entre 5 y 25 elementos, sin distinguir tipo de elemento.
- Podrían soportarse entre 4 y 6 dispositivos hardware, entre 8 y 12 software (incluyendo apps móviles, IA y Cloud) y entre 2 y 4 chips y componentes electrónicos.
- Dos respuestas señalaron que podrían atenderse 3 proyectos. Una de ellas detallaba que podrían ser 2 de IoT y otro de IA

Los tiempos medios de auditoría también dependerán de la naturaleza del objeto de la prueba y de la prueba en sí. En un caso, se planteó un tiempo típico de 6 a 12 meses. En el resto, los tiempos indicados fueron mucho menores, encontrándose los valores más comunes por debajo de 1 mes. En dos casos, se distinguió entre distintos tipos de elementos a probar, indicándose:

- Hardware: Una respuesta indicó entre 3 y 15 días. La otra, de 2 a 8 semanas.
- Software: Una indicó entre 3 y 8 días. La otra, de 2 a 6 semanas.
- IA : Una indicó entre 3 y 10 días. La otra, de 2 a 6 semanas
- Chips y componentes: La respuesta que los mencionó indicó de 4 a 12 semanas.
- Productos completos integrados: La respuesta que los mencionó indicó de 2 a 5 días.

- Comunicaciones: La respuesta que los mencionó indicó de 2 a 10 días.

La duración de todas las etapas necesarias para la puesta en marcha del laboratorio, incluyendo desde la planificación del proceso hasta las pruebas de aceptación, osciló, según respuesta, entre poco más de 1 mes y 24 meses. Los valores más comunes estuvieron comprendidos en el rango entre 5 y 12 meses. En uno de los casos, se indicó que, aunque el proceso para obtener las acreditaciones necesarias supondría entre 3 y 6 meses, el laboratorio podría comenzar a funcionar sin ellas para aquellas actividades en que no son precisas (empezaría a funcionar en entre 2 y 5 meses sin esas acreditaciones)

## 3.7. Costes

Cuatro de las respuestas no incluyeron información acerca de los costes asociados al laboratorio.

Otra planteó un modelo de laboratorio para 5G con un modelo basado en una instalación de equipamiento y unos servicios iniciales, que supondrían un coste de 588.162,00 euros para cuatro años, acompañados de la prestación de servicios puntuales mediante paquetes de horas con su correspondiente coste.

Otra no contemplaba los costes de personal. Solo los de equipamiento y consumibles. Una aproximación del coste de este equipamiento (con mención de elementos concretos) y consumibles, alcanza los 4.532.500,00 euros para dos años.

Se realizó también una evaluación del coste que supondría la instalación y el funcionamiento del laboratorio durante sus dos primeros años de existencia para las otras 3 respuestas que incluyeron datos al respecto, Los costes oscilaron entre algo más de 30.000 euros y unos 840.000 euros, con un promedio de 472.924 euros.

En todo caso, debe señalarse que las respuestas obtenidas fueron orientativas y no se proporcionaba información completa y exhaustiva sobre todos los posibles tipos de gastos. En particular, al no preguntarse de forma expresa en el formulario, solo una de ellas incluía los costes del alquiler y acondicionamiento del espacio necesario, que sería:

- 12-16 €/$m^2$ de alquiler mensual
- 100-200 €/$m^2$ para el acondicionamiento inicial (una sola vez)

## 3.8. Observaciones finales

Las respuestas obtenidas en la consulta preliminar de mercado tienen un alto grado de heterogeneidad, reflejando unas propuestas que parten de distintos supuestos y enfoques. Todo ello refleja la existencia de diversos mercados objetivo, diferentes áreas de actividad y variadas orientaciones y aproximaciones al ámbito de la ciberseguridad.

Al mismo tiempo, esta diversidad, de no abordarse de forma apropiada, podría constituir un riesgo significativo para el éxito del Laboratorio de Ciberseguridad. No solo por las dificultades que pudiera

suponer su dimensionamiento y la elección inicial de equipamiento y servicios, sino también porque, al tratarse de un entorno en continua evolución, podría comprometerse la capacidad del Laboratorio para adaptarse a las transformaciones que experimentará la tecnología y el mercado en los próximos años. Además, debe tenerse en cuenta que, como parte de ese entorno, se está produciendo una intensa actividad en el ámbito de la normativa y de los estándares aplicables

Los costes de equipamiento, puesta en marcha y funcionamiento del Laboratorio, por otro lado, serían altos, lo que incrementa y hace más significativos, si cabe, los riesgos anteriormente citados. Además, cobra especial importancia la viabilidad del proyecto a largo plazo, pues un inversión de esta magnitud debería servir de punto de partida a una iniciativa destinada a tener unos efectos duraderos y profundos.

Por todo lo anterior, para el diseño, la puesta en marcha y el funcionamiento del Laboratorio sería necesaria una entidad (o, en su caso, varias) que presentara las siguientes características:

- Tener conocimiento de la tecnología y del sector tecnológico y su posible evolución.
- Ser capaz de abordar el proyecto desde distintas perspectivas de forma simultanea y crear una solución que se pueda adaptar de forma continuada en el tiempo a los cambios futuros.
- Mantener el necesario grado de independencia con respecto a los diferentes intereses y visiones que pudieran tener distintos agentes del mercado y entidades del sector.
- Ser capaz de crear sinergias con distintos agentes del mercado y entidades del sector, de modo que se mejore las capacidades del Laboratorio y su adaptación a las necesidades que pudieran producirse en todo momento.

EL CONSEJERO TÉCNICO
ENRIQUE RANDO GONZÁLEZ