**Número de expediente SE744000NS2024096**

# Pliego de prescripciones técnicas particulares del contrato de Servicio para la investigación en seguridad de dispositivos IoT en el marco de la Cátedra CARISMÁTICA.

Con la presentación de la oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego, que tienen la consideración de especificaciones mínimas y de obligado cumplimiento.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará excluida de la licitación.

## 1. Objeto del contrato o necesidad a cubrir

El presente Pliego tiene por objeto establecer las prescripciones técnicas particulares que regirán la realización de la prestación del Servicio para la realización de un proyecto de investigación y desarrollo en el campo de la seguridad de dispositivos IoT en el sector de la salud en el marco de la Cátedra CARISMÁTICA de Ciberseguridad, definiendo así sus cualidades.

El citado proyecto se enfoca en abordar desafíos críticos relacionados con la detección temprana de brechas de seguridad en dispositivos IoT y el análisis forense de los mismos en caso de un ataque exitoso y la colaboración para el desarrollo y promoción de la ciberseguridad.

### Características Mínimas Generales

La contratación implica la realización de una investigación exhaustiva en seguridad IoT en entornos de atención médica, incluyendo la revisión del estado del arte y la identificación de áreas clave de enfoque.

Se requiere el desarrollo de algoritmos de detección de anomalías eficientes para identificar actividades sospechosas o comportamientos irregulares en dispositivos IoT en tiempo real.

Además, se necesita la implementación de un prototipo de soluciones propuestas que demuestren la eficacia en la detección de anomalías y la recopilación de datos forenses en dispositivos comprometidos.

La empresa adjudicataria debe proporcionar documentación técnica detallada que respalde las investigaciones, el prototipo implementado y los resultados del proyecto. Se requerirá acceso a un laboratorio con capacidades de cómputo de alto rendimiento para el desarrollo de sistemas de inteligencia artificial y ciberseguridad. Todas las prestaciones deben cumplir con los estándares de seguridad de datos en el sector de la salud. El proyecto debe contribuir al avance de la ciberseguridad en el campo de la

salud y mejorar la protección de los datos y la privacidad de los pacientes en entornos IoT.

**Temporalidad**

Todas las actuaciones se deberán iniciar dentro de los primeros quince (15) días desde la fecha del contrato y finalizarse a 31 de diciembre de 2025.

## 2. Actividades y funciones de la empresa contratista

Las funciones que debe asumir la empresa contratista son las siguientes:

- Elaboración y presentación de un plan de investigación detallado, incluyendo una revisión exhaustiva del estado del arte en seguridad IoT aplicados a la seguridad de redes de datos en entornos de Salud.
- Implementación del prototipo de soluciones propuestas y evaluación de su rendimiento en términos de seguridad, privacidad y eficiencia.
- Documentación de los resultados de la investigación en forma de un artículo científico, listo para ser presentado en conferencias o revistas especializadas en el campo de la seguridad.
- Envío de al menos un artículo asociado a esta tarea de investigación en una conferencia relevante o revista especializada, asegurando la contribución de conocimiento a la comunidad científica y la difusión de los avances realizados en el campo de estudio.
- Organización de al menos una conferencia o evento tipo hackaton, de forma conjunta con los otros miembros del proyecto.

La oferta que presente la empresa licitadora deberá abarcar la totalidad de las actividades y funciones especificadas en el presente pliego y en el Pliego de Cláusulas Administrativas Particulares, siendo todas ellas obligatorias para la admisión de las propuestas.

## 3. Requerimientos técnicos generales obligatorios de la prestación y/o rendimiento o exigencias funcionales de la prestación

La empresa contratista dispondrá de los suficientes medios técnicos, materiales cualitativos y personales para desarrollar las labores objeto de este contrato.

La prestación regulada en el presente pliego deberá ajustarse, al menos, a los siguientes requisitos técnicos:

- Capacidad para desarrollar algoritmos de detección de anomalías.
- Experiencia en el uso de herramientas como OpenUEBA para analizar patrones de comportamiento.
- Habilidad para investigar y desarrollar técnicas específicas para la recopilación y el análisis forense de datos en dispositivos IoT.
- Acceso a un laboratorio con capacidades de computación de alto rendimiento para el desarrollo de sistemas de inteligencia artificial y ciberseguridad.

En términos de rendimiento o de exigencias funcionales, las prestaciones de este contrato tendrán que alcanzar los siguientes hitos:

- Desarrollo de Algoritmos de Detección de Anomalías: El contratista (I2CAT) deberá desarrollar algoritmos de detección de anomalías que sean capaces de analizar el tráfico de red en entornos de dispositivos IoT en el sector de la salud. Estos algoritmos deben ser eficientes y efectivos en la identificación proactiva de actividades sospechosas o comportamientos irregulares.

- Implementación de Herramientas de Análisis de Comportamiento: Se requerirá que el contratista utilice herramientas como OpenUEBA, actualmente en desarrollo por la Fundación I2CAT, para analizar patrones de comportamiento y construcción de perfiles de comportamiento de los dispositivos IoT. Las prestaciones de este contrato deben incluir la implementación y configuración efectiva de estas herramientas.

- Técnicas Específicas de Análisis Forense: El contratista deberá investigar y desarrollar técnicas específicas para la recopilación y el análisis forense de datos en dispositivos IoT comprometidos. Estas técnicas deben permitir la extracción segura de datos de dispositivos afectados, la identificación de modificaciones maliciosas y la recuperación de evidencias digitales de manera efectiva.

- Acceso a Capacidades de Computación de Alto Rendimiento: Dado que el proyecto implica tareas de desarrollo de sistemas de inteligencia artificial y ciberseguridad, el contratista debe tener acceso a un laboratorio con capacidades de computación de alto rendimiento. Este laboratorio debe ser capaz de desplegar entornos aislados ad-hoc para asegurar la seguridad de los proyectos y garantizar un rendimiento óptimo.

- Cumplimiento de Estándares de Seguridad de Datos en Salud: Todas las prestaciones de este contrato deberán cumplir con los estándares de seguridad de datos en el sector de la salud para garantizar la integridad y privacidad de la información de los pacientes.

- Generación de Documentación Detallada: El contratista deberá generar documentación detallada de todas las tareas realizadas, incluyendo la

descripción de los algoritmos, herramientas, técnicas y procesos desarrollados. Esta documentación debe ser clara y completa.

- Contribución al Avance de la Ciberseguridad en el Sector de la Salud: El contratista debe demostrar un compromiso sólido en contribuir al avance de la ciberseguridad en el campo de la salud y mejorar la protección de los datos y la privacidad de los pacientes en un entorno cada vez más conectado.

- Llevar a cabo acciones de comunicación y difusión de información y noticias sobre las actividades realizadas por la Cátedra de ciberseguridad en diversos medios de comunicación: prensa, radio, televisión, con el fin de lograr los siguientes objetivos:

  - Maximizar el impacto alcanzado por las actuaciones y los resultados de la cátedra.
  - Incrementar la conciencia sobre la cultura de la ciberseguridad, particularizado en el entorno sanitario.
  - Promover buenas prácticas (higiene de la ciberseguridad).

### 3.1 Paquetes de trabajo, tareas y entregables

| PT0: Gestión del proyecto | Duración estimada: todo el proyecto. |
|---|---|
| **Descripción del paquete de trabajo:**<br><br>Gestión del proyecto, coordinación de las actividades, planificación y control; tanto de los aspectos técnicos como financieros. El jefe de proyecto asegura que el proyecto alcanza los objetivos marcados y actúa como punto de contacto del proyecto entre todos los equipos | |
| **Tareas:** | |
| • T0.1 Reuniones del proyecto<br>• T0.2 Seguimiento del proyecto<br>• T0.3 Documentación | |
| **Entregables:** | |
| • E0.1 Documentación inicial del proyecto<br>• E0.2 Planificación del proyecto. | |

| PT1: Plan de investigación | Duración estimada: todo el proyecto. |
|---|---|
| **Descripción del paquete de trabajo:**<br><br>Exhaustiva revisión de la literatura para establecer una base sólida para la investigación. Desarrollo de un marco teórico y definición de los objetivos generales y específicos de la investigación. Además, también se incluye el diseño de la metodología de la investigación, identificando las herramientas y técnicas necesarias para recopilar y analizar los datos. Finalmente, se desarrolla y se envía a una conferencia relevante o revista especializada un artículo científico asociado a la tarea de investigación. | |
| **Tareas:** | |
| • T1.1 Revisión de la literatura relacionada con el tema de investigación<br>• T1.2 Desarrollo de un marco teórico sólido<br>• T1.3 Definición de los objetivos<br>• T1.4 Diseño de la metodología de investigación<br>• T1.5 Cronograma detallado para la ejecución del proyecto<br>• T1.6 Investigación<br>• T1.7 Desarrollo de un artículo científico | |
| **Entregables:** | |
| • E1.1 Plan de investigación detallado<br>• E1.2 Artículo científico | |

| PT2: Definición y desarrollo del prototipo | Duración estimada: 12 meses |
|---|---|
| **Descripción del paquete de trabajo:**<br><br>Conceptualización y desarrollo del prototipo de la solución propuesta en la investigación. Definición de los requisitos del prototipo, identificando las características clave y funcionalidades necesarias. A continuación, se procederá con el desarrollo del prototipo, utilizando las herramientas y tecnologías adecuadas según la naturaleza de la investigación. | |

| Tareas: |
| --- |
| • T2.1 Definición y análisis del prototipo<br>• T2.2 Desarrollo iterativo del prototipo<br>• T2.3 Documentación del código y la arquitectura |
| **Entregables:** |
| • E2.1 Diseño del prototipo<br>• E2.2 Prototipo funcional<br>• E2.3 Documentación del código |

| PT3: Test del prototipo | Duración estimada: 8 meses |
| --- | --- |
| **Descripción del paquete de trabajo:**<br><br>Validación del prototipo. Diseño de pruebas específicas para verificar el cumplimiento de los requisitos establecidos en el PT4. Análisis de los resultados de las pruebas, identificando posibles mejoras y ajustes necesarios en el prototipo. | |
| **Tareas:** | |
| • T3.1 Testeo del prototipo<br>• T3.2 Análisis de los resultados: mejoras y corrección de errores | |
| **Entregables:** | |
| • E3.1 Casos de prueba<br>• E3.2 Informes de pruebas con resultados y su evaluación | |

| PT4: Organización de eventos | Duración estimada: totalidad del proyecto. |
| --- | --- |

| |
|---|
| **Descripción del paquete de trabajo:**<br><br>Durante la ejecución de la cátedra se colaborará en la organización de actividades de diseminación tipo workshop, congreso o hackathon. |
| **Tareas:** |
| • T4.1 Generación de los enunciados y material asociado.<br>• T4.2 Ejecución de la hackaton 2025.<br>• T4.3 Actividades de difusión en redes sociales y medios corporativos. |
| **Entregables:** |
| • E4.1 Informe de la hackaton 2025. (Topic: Cybersecurity and Health) |

### 3.2 Mecanismos de verificación de cumplimiento de los distintos indicadores

La empresa contratista estará obligada a facilitar el mecanismo de verificación de cumplimiento de los distintos indicadores, aportando de forma anual un documento de síntesis que justifique debidamente el cumplimiento satisfactorio del hito. Este documento de síntesis incluirá una referencia a en qué plazos y condiciones se ha cumplido el hito, además de pruebas y evidencias concretas sobre el cumplimiento de las actuaciones descritas en este pliego.

### 3.3 Imagen y publicidad

La empresa contratista, siempre que hable de la actuación, deberá hacer mención de que las actuaciones objeto de este contrato se hacen en colaboración con la Universitat Politècnica de Catalunya y deberá informar al público de la participación de la Unión Europea y financiación a través del Plan de Recuperación, Transformación y Resiliencia.

En concreto, en la documentación que se desarrolle al ejecutar las actuaciones en virtud del contrato (como placas, carteles, cuadernillos, notas informativas o de cualquier otro tipo) se deberá exhibir de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga (traducida a las lenguas locales cuando proceda) financiado por la Unión Europea - NextGenerationEU", junto al logo del PRTR, disponible en el link https://planderecuperacion.gob.es/identidad-visual.

### 3.4 Obligaciones de la empresa contratista

La empresa contratista se compromete a cumplir, con carácter general, a cumplir cuantas disposiciones comunitarias y nacionales le resulten aplicables como destinatarias de las actuaciones cofinanciables, así como cumplir las siguientes obligaciones:

- Permitir y facilitar que se puedan realizar las auditorías y comprobaciones necesarias para verificar el cumplimiento de la normativa aplicable.

- Conservar la documentación relacionada con las actuaciones objeto del presente contrato que, dada su naturaleza, le corresponda custodiar conforme al artículo 132 del Reglamento (UE, Euratom) n. º 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión.

- Aplicar medidas antifraude eficaces y proporcionadas, en su ámbito de gestión, sobre el cumplimiento de la normativa aplicable al presente convenio, así como evitar la doble financiación y la falsificación de documentos. También se comprometen a comunicar al Servicio Nacional de Coordinación Antifraude (SNCA) aquellos hechos que pudieran ser constitutivos de fraude o irregularidad.

- Que las actuaciones que se ejecuten en virtud del contrato respetarán el principio de «no causar un perjuicio significativo al medio ambiente» (principio do no significant harm - DNSH) en cumplimiento con lo dispuesto en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, y su normativa de desarrollo, en particular el Reglamento (UE) 2020/852, relativo al establecimiento de un marco para facilitar las inversiones sostenibles y la Guía Técnica de la Comisión Europea (2021/C 58/01) sobre la aplicación de este principio, así como con lo requerido en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del PRTR.

- Garantizar la mutua proporción de los datos de identificación de aquellos contratistas y subcontratistas que, en cumplimiento de la normativa de contratación pública, reciban fondos con cargo al presente Convenio.

## 4. Formas de seguimiento y control de la ejecución de las condiciones

La empresa contratista debe designar a una persona responsable a quien encargar la gestión de la ejecución del contrato y que deberá garantizar la calidad de la prestación objeto de este pliego, tratando directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego con la persona interlocutora designada por el órgano de contratación.

Las personas referidas anteriormente se reunirán con una periodicidad mínima mensual para supervisar, controlar y tratar cualquier aspecto vinculado con el desarrollo del contrato, a fin de asegurar que el mismo se está ejecutando conforme a lo establecido en el presente pliego.

Seguimiento general del proyecto:

- Reuniones periódicas: Programar reuniones regulares entre las partes contratantes para revisar el progreso del proyecto y discutir cualquier problema o desviación. Estas reuniones proporcionan una plataforma para la comunicación y la resolución de problemas en tiempo real.

- Informes de estado: Requerir informes de estado periódicos por parte del contratista para documentar el progreso, los hitos alcanzados y cualquier problema identificado. Estos informes deben incluir métricas clave y datos relevantes para evaluar el desempeño.

- Indicadores clave de rendimiento (KPI): Establecer KPI específicos que reflejen las metas y objetivos del contrato. Los KPI permiten medir el rendimiento y evaluar si se están cumpliendo las condiciones del contrato.

- Revisión de entregables: Evaluar regularmente los entregables o productos intermedios proporcionados por el contratista para asegurarse de que cumplan con las especificaciones y los estándares acordados en el contrato.

- Sistema de seguimiento de problemas: Implementar un sistema para registrar y dar seguimiento a problemas, quejas o disputas que surjan durante la ejecución del contrato. Esto facilita su resolución y documentación.

A los efectos anteriores, se evaluará el seguimiento y control del cumplimiento de cada requerimiento técnico de la siguiente manera:

- Elaboración y presentación de un plan de investigación detallado
    - Fecha de entrega del plan de investigación.
    - Grado de cobertura de la revisión exhaustiva del estado del arte en seguridad IoT en entornos de salud (porcentaje de relevancia de la revisión).
    - Número de referencias y fuentes utilizadas en la revisión.

- Implementación de un prototipo de soluciones propuestas
    - Fecha de entrega del prototipo.
    - Eficiencia de las soluciones implementadas en términos de detección de anomalías (porcentaje de éxito).
    - Rendimiento de las soluciones en cuanto a uso eficiente de recursos computacionales (por ejemplo, consumo de CPU y memoria).

- Documentación de los resultados de la investigación en forma de un artículo científico
    - Fecha de entrega del artículo científico.
    - Nivel de originalidad del artículo (medido por la identificación de nuevas aportaciones en el campo de seguridad IoT en salud).

- Aceptación del artículo en conferencias o revistas especializadas.

- Envío de al menos un artículo asociado a esta tarea de investigación
  - Fecha de envío del artículo a la conferencia o revista.
  - Aceptación del artículo por la conferencia o revista.
  - Contribución del artículo a la comunidad científica (número de citas, impacto en el campo).

- Implementación efectiva de herramientas como OpenUEBA
  - Correcta configuración de OpenUEBA para el análisis de patrones de comportamiento.
  - Eficiencia de OpenUEBA en la construcción de perfiles de comportamiento de los dispositivos IoT (porcentaje de éxito en la identificación de patrones).

- Desarrollo de técnicas específicas de análisis forense
  - Fecha de entrega de las herramientas de análisis forense desarrolladas.
  - Capacidad de las herramientas para extraer datos de dispositivos comprometidos de manera segura (precisión y velocidad).
  - Efectividad en la identificación de modificaciones maliciosas y recuperación de evidencias digitales.

- Acceso a capacidades de computación de alto rendimiento
  - Disponibilidad y tiempo de acceso a las capacidades de cómputo de alto rendimiento.
  - Estabilidad y disponibilidad de los entornos aislados ad-hoc.

Estas métricas específicas ayudarán a evaluar el desempeño y el cumplimiento de las tareas y actividades en el proyecto, así como a medir la eficacia de las soluciones y herramientas desarrolladas por el contratista en relación con los requerimientos técnicos y los objetivos del proyecto.

## 5. Documentación técnica a aportar por la empresa adjudicataria

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si ésta se convierte en la adjudicataria.

A fin de acreditar el cumplimiento de cada especificación técnica exigida en este pliego, la empresa adjudicataria deberá aportar la siguiente documentación:

- Memòria del Plan de Investigación Detallado: Deberá proporcionar el plan de investigación detallado, que incluya la revisión exhaustiva del estado del arte en seguridad IoT en entornos de salud, con una descripción completa de las fuentes de información utilizadas y la metodología de investigación.

- Listado y detalle del conjunto de actuaciones de difusión realizadas.

- Listado oficial del estado de los Artículos Enviados y/o Conferencias realizadas: Para cada artículo enviado a conferencias o revistas, se requerirá la documentación de seguimiento que incluya el artículo, la confirmación de envío, pruebas de aceptación, o cualquier revisión o comentarios recibidos.

- Certificación del representante legal con detalle de los gastos incurridos. Este certificado indicará, de forma expresa, los registros o archivos donde se encuentra custodiada o depositada la documentación justificativa y los departamentos y/o personas responsables de la misma. Esta certificación se acompañará de las justificaciones de los gastos en forma de facturas y transferencias realizadas. En el caso de las horas de dedicación para el personal propio, deberá incluirse el coste asociado a esa dedicación, acompañando la justificación en forma de nóminas o documentos equivalentes.

El Responsable del contrato,

Barcelona, a la fecha de la firma electrónica