

MEMORIA JUSTIFICATIVA DEL CONTRATO

IDENTIFICADOR DOCUMENTO INI-2022-50	IDENTIFICADOR UNIVERSAL	PLANTILLA L9/17-INI
---	-------------------------	------------------------

DESCRIPCIÓN Memoria justificativa - Servicios I+D en tecnologías 6G, en el marco del Proyecto CERBERUS - Bloque OPIs	FECHA DE EMISIÓN 14 / 10 / 2022
---	------------------------------------

CUADRO RESUMEN

OBJETO Prestación de servicios de Investigación y Desarrollo en tecnologías 6G, en el marco del Proyecto Coordinado CERBERUS: Seguridad Dinámica y Gestión sobre Redes Virtualizadas Distribuida, conforme al Real Decreto 1040/2021. Componentes de validación, simulación y soporte al despliegue y evaluación.	
UNIDAD ADMINISTRATIVA E096 INGEN.INFORMACIÓN Y COMUNICACIONES	
RESPONSABLE ANTONIO FERNANDO SKARMETA GOMEZ CATEDRÁTICO DE UNIVERSIDAD INGEN.INFORMACIÓN Y COMUNICACIONES	
RESPONSABLE SENEA CORBALAN GARCIA La Vicerrectora de Investigación VICERRECTORADO DE INVESTIGACIÓN	
LOTES No	TEXTO JUSTIFICACIÓN LOTES En base al requerimiento de las funcionalidades anteriores, el presente contrato de servicios se ha definido en un único lote ya que el contenido está perfectamente identificado como el soporte de los sistemas de validación, simulación y soporte a al despliegue y evaluación.

OBJETO DEL CONTRATO:

El objeto de este contrato es la prestación de servicios de Investigación y Desarrollo en tecnologías 6G, en el marco del Proyecto Coordinado CERBERUS: Seguridad Dinámica y Gestión sobre Redes Virtualizadas Distribuida, conforme al Real Decreto 1040/2021. Componentes de validación, simulación y soporte al despliegue y evaluación.

CERBERUS persigue como principal objetivo proporcionar un framework de administración de seguridad cognitivo, robusto, práctico y adaptable a los eventos futuros. Este framework se basará en técnicas de Inteligencia Artificial (IA) preservando la privacidad para monitorizar, predecir, mitigar y prevenir riesgos y ataques sobre la infraestructura IT. Entre las infraestructuras objetivo se encuentran aquellas que engloban tanto el Internet de las cosas (IoT) y las denominadas SmartCities, así como infraestructuras de comunicaciones 5G, haciendo especial énfasis en las nuevas tendencias orientadas hacia 6G.

Para desarrollar dicho framework se requiere el diseño, definición, implementación y evaluación de dos subcomponentes del sistema CERBERUS que permitan proveer de soluciones en dos ámbitos de investigación del proyecto que serán integrables en el framework general:

- Sistemas de Orquestación Inteligente para la gestión distribuida de políticas y servicios de seguridad y el despliegue de contramedidas

TENIENTE FLOMESTA, S/N . 30003 - MURCIA

Código seguro de verificación: RUxBMiTf-jI1vYUX1-bgAy0Ryz-YAY3Vo8d

Página 1 de 5

Este es un documento administrativo electrónico emitido por la Universidad de Murcia. Su autenticidad puede ser contrastada a través de la siguiente dirección: <https://sede.um.es/validador/>

MEMORIA JUSTIFICATIVA DEL CONTRATO

IDENTIFICADOR DOCUMENTO INI-2022-50	IDENTIFICADOR UNIVERSAL	PLANTILLA L9/17-INI
---	-------------------------	------------------------

- Sistema de monitorización, gestión de datos y compartición para la gestión inteligente de amenazas y contramedidas de seguridad y el uso de técnicas de IA

DIVISIÓN EN LOTES:

En base al requerimiento de las funcionalidades anteriores, el presente contrato de servicios se ha definido en un único lote ya que el contenido está perfectamente identificado como el soporte de los sistemas de validación, simulación y soporte a al despliegue y evaluación.

Lote Componentes de validación, simulación y soporte al despliegue y evaluación.

NECESIDAD, IDONEIDAD Y EFICIENCIA DEL CONTRATO:

- Componente: Componente 15 - Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G.
- Medida del componente: C15.I6 - Despliegue del 5G
- Etiquetado climático: sin etiqueta
- Proyecto: CERBERUS: Seguridad Dinámica y Gestión sobre Redes Virtualizadas Distribuida

- Convocatoria: Real Decreto 1040/2021, de 23 de noviembre, por el que se regula la concesión directa de una subvención a centros y fundaciones públicos de investigación y universidades públicas españolas para la realización de proyectos innovadoras en el despliegue de las tecnologías 5G avanzado y 6G, en el marco del Plan de Recuperación, Transformación y Resiliencia.

- Plan de medidas antifraude y anticorrupción aprobado por Consejo de Gobierno el 26 de enero de 2022

Para conseguir sus objetivos CERBERUS se ha descompuesto en varios subproyectos:

- Gestión de seguridad automatizada en redes 5G/B5G mediante la aplicación del modelo de "closed-loop" basado en arquitecturas ZSM (CERBERUS_ZEUS) TSI-063000-2021-36
- Soporte a la automatización de la seguridad mediante la gestión inteligente de amenazas y contramedidas de seguridad (CyberThreat Intelligence) y la compartición de conocimiento multioperador (CERBERUS_HERMES) TSI-063000-2021-44
- Orquestación automática y reactiva de amenazas y contramedidas de seguridad inter-dominio e intradominio mediante la reprogramación del plano de datos (CERBERUS_HADES) TSI-063000-2021-62
- Despliegue y evaluación de la solución en el ámbito de Smart Campus (CERBERUS_HEFESTO) TSI-063000-2021-45

En la convocatoria y posterior Real Decreto 1040/2021, de 23 de noviembre de concesión, se establece se requiere que de forma complementaria a la investigación que realice la Universidad de Murcia, los beneficiarios de la subvención estarán obligados a subcontratar el 70 por ciento de los fondos recibidos respetando el principio de libre concurrencia y con arreglo a los siguientes requisitos:

TENIENTE FLOMESTA, S/N . 30003 - MURCIA

Código seguro de verificación: RUxBMiTf-jI1vYUX1-bgAy0Ryz-YAY3Vo8d

Página 2 de 5

Este es un documento administrativo electrónico emitido por la Universidad de Murcia. Su autenticidad puede ser contrastada a través de la siguiente dirección: <https://sede.um.es/validador/>

MEMORIA JUSTIFICATIVA DEL CONTRATO

IDENTIFICADOR DOCUMENTO INI-2022-50	IDENTIFICADOR UNIVERSAL	PLANTILLA L9/17-INI
---	-------------------------	------------------------

- Un mínimo del 60 por ciento a empresas que hayan demostrado experiencia en proyectos de I+D+i de excelencia en tecnologías avanzadas de redes móviles.
- Un mínimo del 15 por ciento a pequeñas y medianas empresas que hayan demostrado experiencia en proyectos de I+D+i de excelencia en tecnologías avanzadas de redes móviles.
- Un máximo del 5 por ciento a centros y fundaciones públicos de investigación y universidades españolas que no hayan sido miembros de consorcios de la 5G PPP, pero que aporten capacidades y tecnologías relevantes para el desarrollo de 6G.

Siguiendo este principio el proyecto CERBERUS para su correcta ejecución ha agrupado dentro de los subproyectos tareas que de forma transversal afectan a la solución del framework y como tal requieren de una especialización de conocimientos que se han identificado.

Este pliego cubre el apartado c) anterior para subcontratar a un centro o fundación pública de investigación o universidad española - que no hayan sido miembros de consorcios de la 5G PPP, pero que aporten capacidades y tecnologías relevantes para el desarrollo de 6G - en el contexto de CERBERUS, al ser adjudicataria deberá incluir en el plan de trabajo el diseño de posibles escenarios de pruebas y validación de los aspectos del framework integrados con la infraestructura Gaia-5G, localizada en el Campus de Espinardo de la Universidad de Murcia y su integración en el proyecto de Smart campus. Deberá además proponer una solución para modelar todo el entorno en 3D para hacer simulaciones que comparan todo con lo real, así como una serie de casos de uso que y sus posibles despliegues que sirvan para demostrar la adecuación y el rendimiento del framework.

En base al requerimiento de las funcionalidades anteriores, el presente contrato de servicios se ha definido en un único lote ya que el contenido está perfectamente identificado como el soporte de los sistemas de validación, simulación y soporte al despliegue y evaluación y su integración en el marco de las investigaciones del equipo de la UMU permitirán completar los objetivos globales definidos en el proyecto y que consisten en:

- Diseño y prototipo de una arquitectura que permita administrar la seguridad de forma automatizada mediante un ciclo de autogestión, incluyendo mecanismos de Inteligencia Artificial extensibles y distribuidos para facilitar la automatización. Dicho diseño está alineado con la propuesta del ETSI ZSM (Zero-Touch Network and Service Management), con el fin de lograr que la intervención humana para la operativa se limite al mínimo posible.
- Proveer soluciones de seguridad contrastada que permitan el nivel de automatización requerido, ofreciendo capacidades de autoprotección y auto-curación a la arquitectura propuesta. En ese sentido, dichas soluciones deberán evitar los problemas de seguridad que puedan introducir las técnicas basadas en IA en cuanto a la superficie de ataque y a la propagación de riesgos. CERBERUS ambiciona no sólo aplicar técnicas y algoritmos de IA ya contrastados sino perseguir la definición de nuevos algoritmos, así como la provisión de una base de conocimiento que pueda servir al entrenamiento de dichos procesos.
- Facilitar, manteniendo la privacidad, mecanismos de colaboración y coordinación para habilitar el intercambio de información de ciberseguridad (CTI) y privacidad en tiempo real entre distintos dominios, permitiendo la gestión y la detección de riesgos así como de ataques informáticos, garantizando a su vez el cumplimiento de las consideraciones a tener en cuenta respecto aspectos legales, éticos, sociales, y de privacidad y seguridad. Estos mecanismos cumplirán desde su diseño con la Regulación General de la Protección de Datos (GDPR), siendo además fácilmente extensibles para adaptarse a nuevos/distintos marcos reguladores, y utilizarán las ventajas de tecnologías Blockchain para identificar y gestionar los datos en el entorno distribuido en el que colaboran e interactúan múltiples dominios de organizaciones.

TENIENTE FLORESTA, S/N . 30003 - MURCIA

MEMORIA JUSTIFICATIVA DEL CONTRATO

IDENTIFICADOR DOCUMENTO INI-2022-50	IDENTIFICADOR UNIVERSAL	PLANTILLA L9/17-INI
---	-------------------------	------------------------

4) Habilitar soluciones adaptables y confiables a las nuevas tecnologías para detectar, analizar y procesar ciberataques de forma automatizada y autogestionada en redes emergentes tales como 5G e IoT, así como en redes futuras, teniendo en cuenta nuevos escenarios como pueden ser los operadores multi-tenant, la movilidad en 5G y la eficiencia de recursos en IoT. Los ciberataques sobre estas redes son inherentemente diferentes respecto a los de las redes IP convencionales, por tanto su gestión debe ser acorde a la complejidad de éste nuevo contexto. En ese sentido, CERBERUS está diseñado para gestionar esta complejidad de forma autónoma e inteligente a través de un ciclo de decisión que toma acciones utilizando motores de IA, alimentado por un sistema de políticas de seguridad. Estas políticas proporcionarán distintos niveles de abstracción que ofrecen un amplio abanico de medidas y contramedidas inteligentes de seguridad aplicables de forma dinámica sobre la infraestructura. Para este fin, se hará uso de entornos virtualizados Cloud y Mobile Edge Computing (MEC), así como de la virtualización de la propia red y su programación dinámica tanto del plano de control como del plano de datos. Este entorno adaptable y dinámico permitirá desplegar y/o configurar de forma proactiva y reactiva nuevas soluciones confiables, dónde dicho factor de confiabilidad será proporcionado por un sistema de reputación.

5) Proporcionar un sistema de reputación que evalúe el rendimiento y confiabilidad de las soluciones desplegadas, así como de la infraestructura y otras entidades como servicios de libre transmisión (OTT) e incluso otros operadores, permitiendo el aprendizaje y por lo tanto la evolución automática del sistema hacia un entorno cada vez más inteligente y robusto. Esta evaluación no solo está enfocada al despliegue de soluciones virtuales sino al análisis de las configuraciones de la infraestructura respecto al objetivo y a la evaluación del dominio donde se despliega/configura. Las distintas soluciones, así como los diversos elementos de la infraestructura se verán auditados continuamente con el fin de alimentar el sistema de reputación, capaz entonces de establecer diversos factores de fiabilidad sobre cada entidad del sistema. Esta auditoría continua será además empleada en los casos en los que el sistema pudiera ser vulnerado para identificar responsabilidades.

6) Crear y desplegar un conjunto de casos de uso en entornos relevantes según el ámbito de aplicación para validar la efectividad y eficiencia del todo el framework, mostrando las ventajas de su uso en varios escenarios de ciberseguridad.

7) Identificar y validar los estándares aplicables y proveer de contribuciones a los cuerpos de estandarización claves con el fin de sostener la estandarización en los sectores de ciberseguridad e IoT. Por ejemplo, validar los nuevos avances sobre la arquitectura basada en ZSM, propuesto por el ETSI, así como la incorporación y aplicación del Manufacturer Usage Description (MUD) propuesto en IETF sobre la solución.

DEPARTAMENTO/SERVICIO/UNIDAD DONDE VAYAN DESTINADOS LOS BIENES, PARA QUIEN SE REALICE EL SERVICIO O BAJO CUYA SUPERVISIÓN SE REALICEN LAS PRESTACIONES:

Departamento de Ingeniería de la Información y las Comunicaciones. Facultad de Informática. Campus de Espinardo

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Sí puede haber tratamiento de datos de carácter personal.

DECLARACIÓN SOBRE AYUDAS DE ESTADO Y DOBLE FINANCIACIÓN:

Realizada la autoevaluación sobre ayudas de Estado y doble financiación, siguiendo instrucciones del Anexo III.D., de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, se concluye que este expediente no está cofinanciado.

DECLARACIÓN DEL PROMOTOR DEL CONTRATO.

TENIENTE FLOMESTA, S/N . 30003 - MURCIA

Código seguro de verificación: RUxBMiTf-jI1vYUX1-bgAy0Ryz-YAY3Vo8d

Página 4 de 5

Este es un documento administrativo electrónico emitido por la Universidad de Murcia. Su autenticidad puede ser contrastada a través de la siguiente dirección: <https://sede.um.es/validador/>

MEMORIA JUSTIFICATIVA DEL CONTRATO

IDENTIFICADOR DOCUMENTO INI-2022-50	IDENTIFICADOR UNIVERSAL	PLANTILLA L9/17-INI
---	-------------------------	------------------------

El objeto y alcance del presente contrato se encuentra perfectamente alineado con la actuación financiada, encontrándose asimismo alineado, con el cumplimiento de cuantos hitos y objetivos se han establecido en los instrumentos jurídicos que lo regulan, manifestando que se trata de un gasto elegible y conforme a la normativa que resulta de aplicación.

El responsable
Firma digital: Antonio Fernando Skarmeta Gómez
Catedrático de Universidad
Ingeniería Telemática

CONFORME:
Firma digital: M^a Senena Corbalán García.
Vicerrectora de Investigación.

IdInternos: 44886631, 44888140. Códigos: 11 288, E096, VICINVES, E326, E096. idPersonas: 1602, 2656. numeroDocumentId: Q3018001B, 28710458H, 77562435H. E-SIN-2022-4703. UNIVERSIDAD DE MURCIA (cód.: UMU). OBJETO DEL CONTRATO [LOGOCERBERUS]DIVISIÓN EN LOTESINFORME NECESIDAD E IDONEIDADDEPARTAMENTO/SERVICIO/UNIDAD DONDE VAYAN DESTINADOS LOS BIENESPROTECCIÓN DE DATOS DE CARÁCTER PERSONALDECLARACIÓN SOBRE AYUDAS DE ESTADO Y DOBLE FINANCIACIÓNDECLARACIÓN DEL PROMOTOR DEL CONTRATOPIe de firma de documentos.

TENIENTE FLORESTA, S/N . 30003 - MURCIA

Código seguro de verificación: RUxBMiTf-jI1vYUX1-bgAy0Ryz-YAY3Vo8d

Página 5 de 5

Este es un documento administrativo electrónico emitido por la Universidad de Murcia. Su autenticidad puede ser contrastada a través de la siguiente dirección: <https://sede.um.es/validador/>