

**Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión
Europea-NextGenerationEU****INFORME JUSTIFICATIVO DEL CONTRATO**
(Para contratos de SERVICIOS)

JUSTIFICACIÓN DE LA NECESIDAD E IDONEIDAD DEL CONTRATO; DEL ESTUDIO ECONÓMICO DEL PRESUPUESTO DE LICITACIÓN; DE LA NO SUBDIVISIÓN EN LOTES; DEL PROCEDIMIENTO DE ADJUDICACIÓN; DE LA CLASIFICACIÓN Y DE LOS CRITERIOS DE SOLVENCIA Y ADJUDICACIÓN, DE LAS CONDICIONES ESPECIALES DE EJECUCIÓN; ASÍ COMO DE LA INSUFICIENCIA DE MEDIOS PARA REALIZAR LA PRESTACIÓN

1.- Objeto del contrato: (art. 99 LCSP)

Servicio de implantación de la herramienta GLORIA del CCN-CERT en la Universidad de Zaragoza como parte del proyecto CIBERSECUZ financiado por el Ministerio de Universidades y por la Unión Europea NextGenerationEU/PRTR, en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea- NextGenerationEU.

2.- Financiación

Proyecto “Actuaciones de Seguridad - UZ” financiado por el Ministerio de Universidades y por la Unión Europea “NextGenerationEU”/PRTR.

Ayuda concedida conforme al Real Decreto 641/2021, de 27 de julio, por el que se regula la concesión directa de subvenciones a universidades públicas españolas para la modernización y digitalización del sistema universitario español en el marco del Plan de Recuperación, Transformación y Resiliencia.

Este contrato está financiado por el Mecanismo de Recuperación y Resiliencia de la Unión Europea, establecido por el Reglamento (UE) 2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un Instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, y regulado según 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.

PROYECTO TRACTOR (COMPONENTE 21): Modernización y digitalización del sistema educativo, incluida la educación temprana 0 a 3 años.

MEDIDA I5: Mejora de infraestructuras, el equipamiento, las tecnologías, la docencia y la evaluación digitales universitarios.

 GOBIERNO DE ESPAÑA	 MINISTERIO DE UNIVERSIDADES		Financiado por la Unión Europea NextGenerationEU	 Plan de Recuperación, Transformación y Resiliencia
100% IVA incluido				
53.845,00 €				

3.- Justificación de no división en lotes (art. 99 LCSP)

La única subdivisión posible sería dividir el expediente en las distintas funcionalidades que deberán integrarse en la herramienta SIEM a instalar. Sin embargo, dicha realización independiente de las

1



diversas prestaciones comprendidas en el objeto del contrato dificultaría la correcta ejecución del mismo desde el punto de vista técnico y aumentaría los tiempos de entrega, cuestión inasumible por la financiación que sufra los costes del expediente.

Además, la coordinación de las distintas tareas a realizar reduciría la calidad del servicio solicitado e incrementaría los tiempos de ejecución debido a las interrelaciones existentes entre las distintas funcionalidades solicitadas y plasmadas en el PPT.

4.- Necesidades e idoneidad a satisfacer mediante el contrato: (art. 28 LCSP) así como el estudio económico del presupuesto de licitación (art. 100.2 LCSP)

Necesidades e idoneidad

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permiten una protección adecuada de la información.

Precisamente el artículo 22 del ENS, establece la obligatoriedad de proteger el perímetro de los sistemas a interconectar, en particular si se utilizan redes públicas, total o parcialmente, y de analizar los riesgos derivados de la interconexión de los sistemas, controlando además su punto de unión.

Seguendo la Guía de Seguridad de las TIC CCN-STIC 811 de interconexión del ENS publicada por el Centro Criptológico Nacional (CCN), la Universidad de Zaragoza (UZ) ha desplegado una Arquitectura de Seguridad que incluye dos firewalls diferentes, estos son de dos fabricantes distintos como se recomienda en la propia guía. Un firewall perimetral que es del fabricante PaloAlto y el firewall interno que es del fabricante Fortinet.

Dicho equipamiento es un elemento capital para la seguridad de la red de la UZ, detrás de los cuales se sitúan no solo los sistemas de información y comunicaciones, sino todos los equipos finales de la UZ. Por todo lo expuesto anteriormente estos sistemas generan cantidades ingentes de eventos de seguridad que deben ser analizados conforme al apartado 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Del mismo modo también hay otros sistemas de vital importancia y que generan información de eventos de seguridad como son los sistemas centrales de autenticación de usuarios, el sistema de monitorización de los servicios TIC de la Universidad de Zaragoza, el sistema de gestión de incidencias, etc. Por consiguiente, el tratamiento de todos estos eventos de seguridad debe realizarse de forma automática por una herramienta software dado que su tratamiento manual resulta imposible por el volumen de información a analizar.

Por todo lo expuesto anteriormente y para poder seguir cumpliendo la arquitectura de seguridad establecida en el ENS se debe proceder a la implantación de un sistema de correlación automatizada de eventos de seguridad. Es de vital importancia que la Universidad de Zaragoza, al igual que otras organizaciones, sean capaces de hacer evolucionar sus mecanismos de detección y respuesta a incidentes, atendiendo a las nuevas tipologías de amenazas existentes hoy en día - de forma específica a la amenaza del secuestro de datos o ransomware - para evitar que dichas amenazas puedan llegar a materializarse. Estos objetivos a cumplir se materializarán gracias a la implantación de sistemas automatizados de correlación de eventos de seguridad.

La gravedad de los incidentes en los que se han visto afectadas Universidades o Administraciones Públicas, ha sido igualmente notable, como pudimos observar en 2021 con los casos del Ministerio de Trabajo, Servicio Público de Empleo, Universidad Autónoma de Barcelona o Universidad de Castilla la Mancha por citar unos cuantos.

El Centro Criptológico Nacional - CCN - en el marco de sus competencias, pone a disposición de las Administraciones Públicas un conjunto de herramientas ofrecidas sin coste de licenciamiento a dichas administraciones, que cuentan con una gran madurez y capacidad técnica. Algunas de estas herramientas se han puesto en marcha en los últimos años en la Universidad de Zaragoza:

- Sonda SAT-INET.
- Plataforma de gestión de ciberincidentes LUCIA.
- Sistema de Ciberinteligencia REYES.
- Gestión de Riesgos PILAR.
- Protección frente a Ransomware mediante uCLAUDIA.

En esta misma línea el CCN ha puesto a disposición de las Administraciones Públicas la herramienta GLORIA. Esta herramienta es un SIEM - Security Information and Event Management - que recibiendo notificaciones de diferentes elementos de seguridad (Firewalls, Antivirus, Directorios de validación, sistema de resolución de nombres de dominio DNS...) es capaz de realizar una correlación automatizada de dichos eventos y generar alertas asociadas. Del mismo modo, GLORIA permite una fácil integración con el resto de herramientas del CCN y que ya se encuentran disponibles en la Universidad de Zaragoza.

Además, tal y como se ha indicado anteriormente, de estos objetivos de carácter técnico, existe una obligación por parte de la universidad de adecuarse al Esquema Nacional de Seguridad, que contempla la medida de seguridad descrita dentro del Marco Operacional - Monitorización del sistema, en su



Código de verificación : f45bb4cbb9b9bdf9



apartado [op.mon.3] de Vigilancia un "Refuerzo R1 - Correlación de eventos", que sería de aplicación a Sistemas de Información de nivel básico y medio de universidades, tal y como queda recogido en el perfil de cumplimiento específico CCN-STIC 881A.

Atendiendo a lo establecido por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en concreto por el artículo 157, relativo a la reutilización de sistemas y aplicaciones de propiedad de la administración, la Universidad de Zaragoza puede optar por el despliegue de la citada plataforma GLORIA y las sondas que incorpora ésta, como una solución complementaria a las actualmente desplegadas con el objetivo de mejorar su capacidad de detección de incidentes.

El proyecto tractor (COMPONENTE 21): *Modernización y digitalización del sistema educativo, incluida la educación temprana 0 a 3 años* y más concretamente su medida 15, *Mejora de infraestructuras, el equipamiento, las tecnologías, la docencia y la evaluación digitales universitarias* está destinado a financiar los costes de adquisición y/o servicios TIC en las universidades públicas españolas. Tal y como se ha establecido en el apartado anterior debido al volumen de información que generan los distintos sistemas de control de acceso en un entorno como la Universidad de Zaragoza se hace necesario el tratamiento y la correlación automatizada de la información de control de acceso y monitorización de los sistemas cortafuegos, autenticación centralizada, gestión de la continuidad, etc.

Para realizar estas tareas es necesaria la contratación de los servicios objeto de este contrato, los cuales están intrínsecamente relacionados con el programa tractor y la media que financia el servicio objeto de este expediente.

La dotación económica total del proyecto asciende a 70.000,00 €, por lo que esta adquisición supone la ejecución del 76,92 % de los fondos asignados a la Universidad de Zaragoza.

Estudio económico del presupuesto de licitación

Para calcular el coste del presente contrato, se ha realizado una prospección de mercado sobre PVP de soluciones comerciales para un nivel de eventos similar al requerido.

La ejecución del contrato que se propone no exige la dedicación en exclusiva al mismo de ninguna persona. Su ejecución supone la implantación del SIEM GLORIA por parte del adjudicatario en la Universidad de Zaragoza, tarea que puede simultanearse con otras labores a desarrollar por los trabajadores asignados a la ejecución del servicio solicitado en este expediente de contratación.

5.- Justificación procedimiento utilizado para la adjudicación

Se propone la utilización del procedimiento abierto para su adjudicación, de acuerdo con lo indicado en el artículo 131.2 de la LCSP, concretamente el procedimiento abierto simplificado previsto en artículo 159.1 de la misma, así como el art.51 RDL 36/2020, de 30 de diciembre, por el que se aprueba medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, por cumplirse las dos condiciones establecidas en los citados artículos, ser un contrato de servicios de valor estimado inferior a 215.000 € y no superar los criterios de adjudicación evaluables mediante juicio de valor previstos el 25% del total.

6.- Plazo de duración, ejecución y posibles prórrogas

Se propone una duración del contrato de cuatro meses de duración para posibilitar la implantación de los servicios a desarrollar por el adjudicatario en la Universidad de Zaragoza y posteriormente recuperar la prestación del servicio mediante personal propio, razón por la cual en el Pliego de Prescripciones Técnicas se contempla la formación asociada al personal de la Universidad de Zaragoza y la devolución de la prestación del servicio.

7.- Clasificación y/o solvencia a exigir a los licitadores: (art. 77-79 Y 86-94 LCSP)

- ☒ De acuerdo con lo establecido en el artículo 77.1.b) LCSP, por tratarse de un contrato de servicios, para los cuales no es exigible la clasificación, los licitadores podrán acreditar su solvencia mediante su clasificación como contratistas de servicios en el grupo o subgrupo y categoría que corresponde al contrato, según lo dispuesto en los artículos 37 y 38 del RGLCAP, o bien mediante el cumplimiento de requisitos específicos de solvencia económica y financiera y técnica o profesional que se exigen según lo dispuesto en los artículos 87 y 90 LCSP.

8.- Criterios de adjudicación: (art. 145-148 LCSP)

Debido a que el objeto del contrato es la prestación de un servicio se hace necesaria la evaluación del proyecto de implantación, el coste y los servicios a prestar por el adjudicatario, tanto en cantidad como en



Código de verificación : f45bb4cbb9bdfdf9



calidad.

Los criterios de evaluación previa suponen 10 puntos, menos del 25% conforme al artículo 159.1.b, y 90 puntos evaluables mediante criterios de evaluación posterior (permitiendo evaluar los costes y la cantidad y calidad de los servicios solicitados) permitiendo a la Universidad de Zaragoza obtener el servicio con mejor relación calidad precio.

Se ha seleccionado como único criterio de evaluación previa las decisiones asociadas al plan de trabajo seleccionado por los distintos licitadores para la prestación del servicio permitiendo en base a dicho plan reducir los plazos de entrega, aumentar la calidad del servicio prestado, simultanear la realización de las tareas asociadas al servicio a prestar.

Se asignan 90 puntos a los criterios de evaluación posterior ponderados del siguiente modo:

- Oferta económica: se le asigna un peso del 70% dado que se ha fijado la herramienta SIEM a integrar en la infraestructura TIC de la Universidad de Zaragoza y los costes en los que incurrirán los distintos licitadores se fundamentarán en el incremento de las prestaciones a proporcionar a la Universidad de Zaragoza.
- Incremento del número de horas de la bolsa ofertadas por cada licitador respecto del mínimo especificado en el Pliego de Prescripciones Técnicas (10%), permitiendo valorar el aumento de los beneficios obtenidos por la universidad.
- Integración con distintos sistemas (10%): firewall perimetral PaloAlto, Telegram, sistemas de directorio LDAP, sistema de monitorización PandoraFMS y sistema de Ticketing OSTicket utilizados por la Universidad de Zaragoza. Posibilitando valorar la incorporación de funcionalidades a la solución propuesta y la calidad de las mismas.

Mediante la evaluación de los criterios de evaluación posterior se valorará la oferta realizada, la mejora en la cantidad y calidad de los servicios que prestará el licitador y la capacidad de integración de la solución ofertada por el servicio objeto del expediente de contratación.

9.- Condiciones especiales de ejecución: (art. 202 y 145 LCSP)

Se establece como condición especial de ejecución del contrato de tipo social o relativas al empleo: garantizar la seguridad y la salud en el lugar de trabajo y el cumplimiento de las condiciones salariales de los trabajadores conforme a los convenios sectoriales y territoriales aplicables. Dicha condición especial de ejecución está vinculada al objeto del contrato en el sentido del artículo 145 LCSP, no es discriminatoria y es compatible con el derecho comunitario.

10.- Insuficiencia de medios: (art. 116.4.f) LCSP)

En cumplimiento del artículo 116.4. f) LCSP y de acuerdo con lo indicado en la recomendación 1/2013, de 27 de febrero, de la Junta Consultiva de Contratación Administrativa de la Comunidad Autónoma de Aragón, esta unidad informa que es necesaria la prestación íntegra del "Servicio de implantación de la herramienta GLORIA del CCN-CERT en la Universidad de Zaragoza como parte del proyecto CIBERSECUZ financiado por el Ministerio de Universidades y por la Unión Europea NextGenerationEU/PRTR, en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea- NextGenerationEU", que la Universidad de Zaragoza no dispone de los medios humanos y materiales necesarios para su realización, y que, por lo tanto, no se está llevando a cabo por empleados públicos. Por todo lo cual se hace necesario recurrir a la contratación externa de estos servicios, los cuales no se encuentran entre las competencias que la Universidad tiene atribuidas.

Documento firmado electrónicamente y con autenticidad contrastable según el artículo 27.3 c) de la ley 39/2015 por el director del área de sistemas del SICUZ, Juan Carlos Xifre Castellot y el Vicegerente de Tecnologías de la Información y Comunicación, Pascual Pérez Sánchez



Código de verificación : f45bb4cbb9b9bdf9