

INFORME DE NECESIDAD E IDONEIDAD

CONTRATO ESPECÍFICO DERIVADO DEL SISTEMA
DINÁMICO DE ADQUISICIÓN 25/2022 SUMINISTRO DE
SOFTWARE DE SISTEMA, DE DESARROLLO Y DE
APLICACIÓN

SUMINISTRO DE LICENCIAS DE HERRAMIENTA DE
PENTESTING Y SIMULACIÓN DE ATAQUES

EXPEDIENTE N.º: 30/2024

Área: Ciberseguridad

1. OBJETO DEL CONTRATO

A. TIPO DE CONTRATO:

- ☐ CONTRATO DE OBRAS
☒ CONTRATO DE SUMINISTROS
☐ CONTRATO DE SERVICIOS

B. OBJETO DEL CONTRATO:

El objeto del presente contrato comprende la de proporcionar a Canal de Isabel II, Sociedad Anónima, M.P., (en adelante Canal), el suministro de licencias de una herramienta de tipo *Breach and Attack Simulation* “BAS”, que permita la realización de *pentesting* y simulaciones de ataques. Con ello se permitirá tener un mayor control sobre las vulnerabilidades de seguridad en los sistemas informáticos de la empresa. Esto permitirá adelantarse a las nuevas amenazas cada vez más avanzadas. Este suministro constará del software necesario y las correspondientes licencias válidas durante el periodo del contrato. Durante la validez de las licencias, el sistema se actualizará de forma automática con las últimas técnicas de ataque disponibles.

C. DIVISIÓN EN LOTES:

- ☒ NO
☐ SÍ

Canal de Isabel II, S.A, M.P. no ha dividido el objeto del contrato en lotes debido a que la realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificultaría la correcta ejecución de este desde el punto de vista técnico, debido a que dichas prestaciones forman parte de un único servicio global.

2. PLAZO DE DURACIÓN O DE EJECUCIÓN

La duración del contrato es de 3 años a contar del día siguiente al de adjudicación del contrato.

3. MEMORIA ECONÓMICA

A. PRESUPUESTO BASE DE LICITACIÓN (PBL)

	BASE	IVA	TOTAL
PBL	360.000,00	75.600,00	435.600,00

Valor estimado del contrato (IVA Excluido): 360.000 €

B. ÁMBITO DE APLICACIÓN

EMPRESA DEL GRUPO	Importe
CANAL DE ISABEL II, S.A., M.P.	360.000,00
TOTAL (Presupuesto Base de Licitación s/ IVA)	360.000,00

C. PARTIDA PRESUPUESTARIA

Gasto:			
CEGE	CUENTA	POSICIÓN	ORDEN
L105000	621200	G/621200/000003	62010663

Línea Estratégica:

* Descripción Línea Estratégica	* Descripción Línea Estratégica
☐ LE01: Asegurar garantía de Suministro	☐ LE07: Transparencia, buen gobierno y compromiso
☐ LE02: Garantizar calidad agua de consumo	☐ LE08: Talento, compromiso y salud profesionales
☒ LE03: Fortalecer continuidad de servicio	☐ LE09: Liderar innovación y desarrollo
☐ LE04: Calidad ambiental y eficiencia energética.	☐ LE10: Sostenibilidad y eficiencia en la gestión
☐ LE05: Cooperación con municipios de Madrid	☐ N/A: No Aplica
☐ LE06: Compromiso y cercanía con usuario	

Plan estratégico 3.3: “Plan de seguridad de la información”

D. ESTIMACIÓN DE DISTRIBUCIÓN PRESUPUESTARIA POR ANUALIDADES

Se detalla a continuación el desglose del importe estimado según la duración del contrato:

AÑO	GASTO	INVERSIÓN	TOTAL (Sin IVA)
2024	120.000,00	0,00	120.000,00
2025	120.000,00	0,00	120.000,00
2026	120.000,00	0,00	120.000,00
TOTAL (Sin IVA)	360.000,00	0,00	360.000,00

E. ¿ESTE CONTRATO ES SUSTITUCIÓN O RENOVACIÓN DE UNO YA EXISTENTE?

- ☐ SI Los datos comparativos figuran en el anexo a este documento.
☒ NO

F. ¿SE ENCUENTRA INCLUIDO EN LA PLANIFICACIÓN PLURIANUAL VIGENTE?

- ☒ SI Código asignado: PCCYII 24-001
☐ NO

4. MEMORIA JUSTIFICATIVA

A. NECESIDAD E IDONEIDAD DEL CONTRATO.

A.1: NECESIDADES QUE SATISFACER:

Canal, considera la seguridad de la información como un pilar fundamental para garantizar la información tratada y los servicios prestados en su aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestiona en el ejercicio de sus competencias.

Las nuevas amenazas de seguridad surgidas durante los últimos años utilizan nuevas técnicas, tácticas y procedimientos de actores de amenazas (*threat actors*) cada vez más avanzados y que disponen de financiación, motivación, e incluso están respaldados por algunos gobiernos y estados nación. Con la automatización e incorporación de la Inteligencia Artificial, los atacantes disponen de nuevas herramientas, más rápidas y eficaces, que les permiten lanzar gran cantidad de ataques y actualizar y mejorar las técnicas de éstos para la evasión de las medidas de protección desplegadas.

Por tanto, es de vital importancia la identificación proactiva de vulnerabilidades para identificar y comprender tanto todos los posibles vectores de ataque como otros posibles fallos en la seguridad relacionados. Por tanto, para que Canal sea capaz de adelantarse a esta nueva tipología de ataques más sofisticados, es necesario disponer de nuevas herramientas tecnológicas avanzadas que permitan identificar los problemas de seguridad de forma preventiva y ayudar no sólo a mantener un adecuado nivel de seguridad, sino a incrementarlo.

A.2: IDONEIDAD DE LA PROPUESTA PLANTEADA:

Actualmente desde el Área de Ciberseguridad, dependiente jerárquicamente de la Dirección de Seguridad, se realizan auditorías de Hacking ético (*pentesting*) sobre los sistemas informáticos existentes de forma manual, si bien los desafíos en ciberseguridad están aumentando en complejidad, ya que tanto los riesgos como las herramientas y técnicas empleadas por los atacantes se han diversificado y avanzado en sofisticación y rapidez.

Para poder mitigar, e incluso anular estas amenazas, se plantea el uso de las últimas herramientas de simulación de ataques y penetración capaces de imitar perfectamente la forma en la que los atacantes realizan sus intrusiones en los sistemas de información, permitiendo adelantarse a ellos e identificar de forma tempranas las debilidades existentes, así como implementar todas las medidas preventivas necesarias de forma rápida, eficaz y eficiente.

Este tipo de pruebas deben poder realizarse de forma automática. Además, la herramienta se actualizará de forma automática durante toda la vigencia de uso de las licencias suministradas, añadiendo nuevas capacidades, como la inclusión de nuevas técnicas, tácticas y procedimientos de ataque que vayan apareciendo durante el tiempo de vigencia del contrato y que puedan ser replicadas por la herramienta.

Dentro de las capacidades que debe proporcionar este tipo de herramientas, se identifica la necesidad de una actualización automática de las nuevas técnicas, tácticas y procedimientos utilizados por los actores de amenazas, la realización del *pentesting* y simulaciones de ataques a la infraestructura interna y la evaluación de los servicios expuestos en Internet, lo que incluye la inspección de información vinculada a Canal, no sólo en Internet, sino también en la *Deep Web* y, específicamente, en la *Dark Web*.

Por último, esta herramienta de simulación de ataques y penetración permitirá a Canal cumplir con lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en su Artículo 8 “Prevención, detección, respuesta y conservación”, su Artículo 10 “Vigilancia continua y reevaluación periódica” y su Artículo 21 “Integridad y actualización del sistema” y, concretamente, con los siguientes requerimientos de seguridad recogidos en su Anexo II:

- 4.1.2 Arquitectura de seguridad [op.pl.2].
- 4.3.3 Gestión de la configuración de seguridad [op.exp.3].
- 4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].
- 4.7.3 Vigilancia [op.mon.3].
- 5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

A.3: JUSTIFICACIÓN DE LA INSUFICIENCIA DE MEDIOS (PARA CONTRATOS DE SERVICIOS):

No aplica.

B. JUSTIFICACIÓN DE LOS VALORES ECONÓMICOS.

Para la justificación del precio base de la licitación, se ha llevado a cabo una evaluación de herramientas licitadas para el sector público. Esta estimación se basa en la información recopilada a partir de los datos de la publicación del contrato en la página oficial de Contratación del Estado, donde está disponible y consultable.

El expediente en el que se basa el presente estudio es en el contrato basado *AST_2023_AMSECCD12, dentro del Acuerdo Marco AST_2022_004* para la prestación de servicios de ciberseguridad con destino a los Departamentos de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos dependientes de la Entidad Pública Aragonesa de Servicios Telemáticos. En esta licitación, se prevé la utilización de una herramienta con características muy similares a las solicitadas en este informe, con un derecho de uso de las licencias de un máximo de 12 meses.

En el citado acuerdo marco, en el punto de la estimación de los precios de las herramientas, se reconoce la dificultad de evaluar el coste de ciertas aplicaciones, ya que éstas son muy específicas y no existen listados de precios públicos.

En base a la experiencia con este tipo de herramientas que disponen de un licenciamiento basado en el número de sistemas a inspeccionar (*end-points*), se estima un coste fijo del despliegue de la propia aplicación al que se le añadirían los costes asociados al soporte, disponibilidad para el mantenimiento, acceso a la actualización automática de los ataques realizados, formación en el uso de la herramienta, etc.

Por otro lado, se estima un coste variable en función del número de *end-points* que permita utilizar, el cual se va reduciendo su coste al aumentar el número de activos. Es difícil tener un valor exacto de la relación existente entre las distintas volumetrías de *end-points*, ya que existen muchas casuísticas y disparidad de tipos y características de *end-points*, lo que incrementa las dificultades del análisis.

El presupuesto base de licitación del citado contrato basado fue de 70.247,93 € IVA excluido y el precio de adjudicación resulto un importe de 68.483,59 € IVA excluido.

En dicho contrato basado, existe un suministro adicional de hardware de alto rendimiento para la ejecución de las capacidades de la solución BAS. Sin embargo, para la presente licitación este tipo de hardware será solicitado al Área de Atención al Usuario de Canal de Isabel II, S.A., M.P. como un equipo informático, por lo que no se tendrá en cuenta ese coste en el presupuesto base de licitación del presente procedimiento de licitación, estimado en unos 2.850 €.

Teniendo en cuenta lo anterior la base del cálculo del precio a tener en cuenta es de 65.633,59 € IVA excluido. Para este caso, se estima una parte fija del 80% y una parte variable de un 20%.

Debido a que la licencia propuesta se basa en 4000 *end-points* frente a los 500 del referido contrato basado, se estima una corrección del coste por cada punto final aplicando un factor de corrección del 0,55.

Coste por <i>end-point</i> (para 500 <i>end-points</i>)	26,25 €
Factor de corrección	0,55
Coste por <i>end-point</i> (para 4000 <i>end-points</i>)	14,44 €

Con estos datos, el coste fijo de implementación sería similar al Contrato basado referido anteriormente (52.506,87 € IVA excluido). El coste variable con la corrección por punto sería de 57.757,57 € IVA excluido, lo que supondría un coste total de 110.264,438 € IVA excluido. A este coste, habría que añadir la funcionalidad adicional de la gestión de la superficie de exposición, relativa a los servicios e información publicados en Internet. Para esta parte, se estima un coste de un 20% adicional sobre el total (dado que no hay especificidad del hardware), obteniendo un coste de 22.052,89 € IVA excluido.

En base a las estimaciones realizadas, se obtendría un coste anual total estimado de 132.317,33 € IVA excluido.

	Coste fijo	Coste variable	Coste solución estándar	Coste funcionalidad adicional superficie de exposición en Internet	Total anual
Contrato basado	52.506,87 €	13.126,72 €	65.633,59 €	0,00 €	65.633,59 €
Estimación	52.506,87 €	57.757,57 €	110.264,44 €	22.052,89 €	132.317,33 €

Considerando que Canal es una empresa de referencia en el sector y el interés de las empresas de ciberseguridad en disponer de referencias sobre sus herramientas en los distintos sectores, se plantea partir de un PBL de 120.000 € anuales, lo que supondría una estimación total de 360.000 € para los tres años de duración del contrato, que es conforme a los precios de mercado. Por tanto, el desglose de los costes directos e indirectos y otros eventuales gastos calculados para la determinación del presupuesto base de licitación en base a precios del mercado es el siguiente:

Costes directos de Personal:	No aplican al ser el objeto del contrato un suministro.
Resto de costes directos:	80% del presupuesto.
Costes indirectos:	No existen
Gastos generales:	13% del presupuesto.
Beneficio Industrial:	07% del presupuesto.

5. PROCEDIMIENTO DE ADJUDICACIÓN

- ☐ ABIERTO
- ☐ NEGOCIADO
- ☐ CONTRATACIÓN BASADA EN ACUERDO MARCO (AM)
- ☒ CONTRATACIÓN ESPECÍFICA DERIVADA DE SISTEMA DINÁMICO DE ADQUISICIÓN (SDA)

EN EL CASO DE PROCEDIMIENTO NEGOCIADO, INDICAR EL SUPUESTO QUE CORRESPONDA:

- ☐ DERECHOS EXCLUSIVOS
- ☐ RAZONES TÉCNICAS
- ☐ DESIERTO ANTERIOR
- ☐ URGENCIA
- ☒ OTROS

EN LOS CASOS DE PROCEDIMIENTO CONTRATOS BASADO EN AM O ESPECÍFICOS DERIVADOS DE UN SDA, IDENTIFICAR EL AM O SDA CORRESPONDIENTE:

Con fecha 12 de julio de 2023, el Área de Planificación y Control de Canal de Isabel II, S.A., M.P. incoó el Informe de Necesidad e Idoneidad del expediente 140/2023 motivando la solicitud de adhesión específica al Sistema Dinámico de Adquisición 25/2022 "SUMINISTRO DE SOFTWARE DE SISTEMA, DE DESARROLLO Y DE APLICACIÓN" del sistema estatal de contratación centralizada (en adelante, "SDA 25/2022").

Una vez realizados los trámites internos necesarios para la adhesión específica al SDA 25/2022, la Dirección General de Racionalización y Centralización de la Contratación acordó, el 19 de octubre de 2023, la adhesión específica de Canal de Isabel II, S.A., M.P. al SDA 25/2022.

Teniendo en cuenta lo anterior, el presente procedimiento de licitación se tramita mediante contrato específico del Lote 4 "Software de ciberseguridad" del referido SDA de conformidad con los pliegos del SDA y sus Instrucciones reguladoras para la contratación específica.

Firmas:

ESCRIBANO
GARCÍA ALBERTO
52128412Q FIRMA

Firmado digitalmente por
ESCRIBANO GARCÍA
ALBERTO - 52128412Q
FIRMA
Fecha: 2024.06.14 11:13:25
+02'00'

Alberto Escribano García
Jefe de Área de Ciberseguridad

Firmado por ***3690** RICARDO
LLORENTE (R:****8808*) FIRMA el día
14/06/2024 con un certificado emitido por SIA
SUB01

Ricardo Llorente Hernán-Gómez
Director de Seguridad