

INFORME DE NECESIDAD E IDONEIDAD

SERVICIOS DE CIBERSEGURIDAD PARA CANAL DE ISABEL II, S.A., M.P.

EXPEDIENTE N.º: 265/2025

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 contrato es la contratación de Servicios de Ciberseguridad, que darán soporte, asesoramiento y apoyo integral al Área de Ciberseguridad, dependiente jerárquicamente de la Dirección de Seguridad, en todo lo relacionado con la gestión de los riesgos de ciberseguridad asociados al desarrollo, mantenimiento y uso de los sistemas de información y de las infraestructuras tecnológicas y de operación de Canal de Isabel II, con el objeto de garantizar la integridad, disponibilidad y confidencialidad de la información propiedad de Canal de Isabel II, S.A., M.P. gestionada en ellos, y principalmente en los sistemas que soportan los servicios prestados por Canal de Isabel II, S.A., M.P. en el ejercicio de sus competencias y potestades administrativas que se encuentran bajo el ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), así como el cumplimiento de los requisitos legales aplicables.

En el Pliego de Prescripciones Técnicas se describen las consideraciones de tipo social, ambiental y de innovación que se han tenido en cuenta para configurar las prestaciones objeto del contrato.

En los documentos referidos en la cláusula 1 del Pliego de Cláusulas Administrativas Particulares (PCAP) se describen las consideraciones de tipo sociales, ambientales y de innovación que se han tenido en cuenta para configurar las prestaciones objeto de los cinco contratos.

C. DIVISIÓN EN LOTES:

☐ NO☒ SÍ

El expediente se divide en TRES (3) LOTES en los cuales se independizan aquellas prácticas que tienen menos dependencias y sinergias entre sí, con el objeto de facilitar la concurrencia y garantizar la correcta ejecución de los aspectos más relevantes de la práctica de la ciberseguridad de manera global.

LOTE 01: CENTRO DE OPERACIONES DE SEGURIDAD (SOC) E INTELIGENCIA DE AMENAZAS (Servicios de Operación de Ciberseguridad, que incluyen la monitorización de los sistemas de información a través de distintas fuentes de reporte de eventos de seguridad, la gestión y operación de dichas fuentes, la normalización y la correlación de eventos para la detección y respuesta ante incidentes de seguridad, el análisis de amenazas a Canal de Isabel II, S.A., M.P. o a sus intereses legítimos a través de la inteligencia de amenazas (*Threat Intelligence*)).

LOTE 02: OFICINA TÉCNICA DE SEGURIDAD (OTS) (Servicios orientados a fortalecer la protección de las infraestructuras de Canal de Isabel II, S.A., M.P. a través de pruebas de seguridad (*pentesting*, auditorías, revisión de configuraciones de seguridad, arquitecturas, capacidades, etc.), con el objeto de mejorar el nivel de seguridad actual de Canal de Isabel II, S.A., M.P. y garantizar que las tecnologías ya implantadas o por implantar tengan una configuración óptima y estén libres de vulnerabilidades).

LOTE 03: ANÁLISIS DE RIESGOS DE ACTIVOS DE INFORMACIÓN, NORMATIVA Y MADUREZ EN CIBERSEGURIDAD (Servicios orientados a la gestión de la gobernanza de la ciberseguridad, análisis de riesgos de los activos de información y cumplimiento normativo en ciberseguridad, incluyendo la definición, mantenimiento, seguimiento del marco normativo interno, el cumplimiento de toda la normativa legal aplicable a la ciberseguridad, elaboración de informes, cuadros de mando y métricas de seguridad, planes de formación y concienciación, y medición de la madurez en ciberseguridad).

Número máximo de lotes a los que un mismo licitador podrá presentar oferta: Los licitadores podrán presentar oferta a los **TRES (3) LOTES**.

Número máximo de lotes de los que un mismo licitador podrá resultar adjudicatario: Cada licitador, individualmente o en UTE, sólo podrá ser adjudicatario de UN (1) lote con el fin de asegurar la capacidad de ejecución en tiempo y forma por parte de las distintas empresas adjudicatarias, y garantizar así la correcta realización de los trabajos encomendados, ya que la adjudicación de más de un lote a un mismo adjudicatario incrementa el riesgo de indisponibilidad de recursos por parte del adjudicatario y un empeoramiento de los servicios prestados. Además, cada lote requiere un alto grado de especialización técnica. La adjudicación de más de un lote a una misma empresa podría diluir esta especialización, comprometiendo la calidad y eficiencia de los trabajos. La especialización es crucial para garantizar que los trabajos se realicen con los estándares más altos y en el menor tiempo posible.

2. PLAZO DE DURACIÓN O DE EJECUCIÓN

El plazo de duración inicial del contrato será de CUATRO (4) años que dará comienzo a partir del día siguiente a la fecha de firma del acta de inicio de los trabajos. Se establece una eventual prórroga de UN (1) año adicional.

3. MEMORIA ECONÓMICA

A. PRESUPUESTO BASE DE LICITACIÓN (PBL)

Lote	BASE	IVA	TOTAL
Lote 1	2.500.000,00 €	525.000,00 €	3.025.000,00 €
Lote 2	1.500.000,00 €	315.000,00 €	1.815.000,00 €
Lote 3	1.000.000,00 €	210.000,00 €	1.210.000,00 €
TOTAL	5.000.000,00 €	1.050.000,00 €	6.050.000,00 €

B. ÁMBITO DE APLICACIÓN

EMPRESA DEL GRUPO	Importe
CANAL DE ISABEL II, S.A. (M.P.)	5.000.000,00 €
TOTAL (Presupuesto Base de Licitación s/ IVA)	5.000.000,00 €

C. PARTIDA PRESUPUESTARIA

Gasto:			
CEBE	CUENTA	POSICIÓN PRESUPUESTARIA	ORDEN
L105000	623001	G/623001/000001	62006403

Línea Estratégica:

*	Descripción Línea Estratégica	*	Descripción Línea Estratégica
☒	LE01: Garantía y continuidad del suministro	☐	LE06: Nuestros profesionales
☐	LE02: Calidad del agua	☐	LE07: Transformación digital e innovación
☐	LE03: Calidad ambiental	☐	LE08: Gestión económico-financiera sostenible
☐	LE04: Transición energética	☐	N/A: No Aplica
☐	LE05: Clientes y sociedad		

D. ESTIMACIÓN DE DISTRIBUCIÓN PRESUPUESTARIA POR ANUALIDADES

D.1 DISTRIBUCION DEL PRESUPUESTO INICIAL:

AÑO	Lote 1	Lote 2	Lote 3	Total (sin IVA)
2026 (2º semestre)	312.500,00 €	187.500,00 €	125.000,00 €	625.000,00 €
2027	625.000,00 €	375.000,00 €	250.000,00 €	1.250.000,00 €
2028	625.000,00 €	375.000,00 €	250.000,00 €	1.250.000,00 €
2029	625.000,00 €	375.000,00 €	250.000,00 €	1.250.000,00 €
2030 (1º semestre)	312.500,00 €	187.500,00 €	125.000,00 €	625.000,00 €
TOTAL (sin IVA)	2.500.000,00 €	1.500.000,00 €	1.000.000,00 €	5.000.000,00 €

D.2 DISTRIBUCION DE LAS PRÓRROGAS:

AÑO	Lote 1	Lote 2	Lote 3	Total (sin IVA)
2030 (2º semestre)	312.500,00 €	187.500,00 €	125.000,00 €	625.000,00 €
2031 (1º semestre)	312.500,00 €	187.500,00 €	125.000,00 €	625.000,00 €
TOTAL (sin IVA)	625.000,00 €	375.000,00 €	250.000,00 €	1.250.000,00 €

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

☒ **SI**
☐ **NO**

SI HA RESPONDIDO SÍ, INDICAR CUÁL/CUÁLES SON LOS CONTRATOS RENOVADOS:

CONTRATO N.º: 5/2021 relativo a "SERVICIOS DE CENTRO DE CIBERSEGURIDAD".

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

☒ SI Código asignado: PCCYII 25 - 245
☐ NO

4. MEMORIA JUSTIFICATIVA

A. NECESIDAD E IDONEIDAD DEL CONTRATO

A.1: NECESIDADES QUE SATISFACER:

Canal de Isabel II, S.A., M.P. considera la ciberseguridad como parte de su estrategia corporativa para garantizar la prestación de los servicios esenciales a los ciudadanos y a la administración pública, mediante la protección adecuada de la información tratada en todos los sistemas de información, y especialmente en los que soportan los servicios prestados por Canal de Isabel II, S.A., M.P. en el ejercicio de sus competencias y potestades administrativas, con el objetivo de asegurar la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad de dicha información.

Canal de Isabel II, S.A., M.P. emprendió en 2010 un proceso para la gestión integral de la seguridad de información realizando en un Plan Director de Seguridad basado en la norma internacional UNE-ISO/IEC 27001 y en las buenas prácticas de la seguridad de la información comúnmente aceptadas a nivel internacional, y que dio como resultado una Política de Seguridad de la Información y Continuidad de Negocio, como piedra angular en el desarrollo de dicho Plan Director de Seguridad, y la definición de un claro objetivo: la reducción de los riesgos en seguridad de la información identificados en el análisis de cumplimiento de la norma ISO/IEC 27002. Para la consecución de este objetivo de reducción del riesgo existente, se identificó un Plan de Acción, detallado en distintas iniciativas en materia de seguridad de la información. Para gestionar dichas iniciativas de manera conjunta, se puso en marcha un comité con funciones específicas en materia de seguridad: el Comité de Coordinación de la Seguridad de la Información (CCSI) que ha evolucionado a un Marco de Gobernanza de la Seguridad, al actual Comité de Seguridad de la Información (CSI) y el Comité de Crisis para dar cumplimiento, principalmente, al Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS).

La creciente complejidad y criticidad de la gestión de la seguridad de la información y de los sistemas de información de Canal de Isabel II, S.A., M.P. que la gestionan y que permiten sostener y desarrollar su actividad, hace imprescindible y necesario evolucionar los actuales servicios de Centro de Operaciones de Seguridad (SOC), Inteligencia de Amenazas (*Threat Intelligence*) y Oficina Técnica de Seguridad (OTS), reorganizarlos de forma más eficiente conforme al nuevo estado del arte y las tendencias en ciberseguridad identificadas para contemplar las nuevas metodologías, tecnologías, tácticas, técnicas y procedimientos, responder con garantías a los nuevos requisitos y complejos retos que se plantean, consolidando así tanto las iniciativas ya implantadas e incorporar nuevas técnicas e iniciativas, teniendo siempre como objetivo el minimizar de forma continua el riesgo existente, incluyendo el de los proveedores, consolidando las bases para el cumplimiento legal vigente (principalmente, el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS)) y la Directiva 2022/2555 del Parlamento Europeo y del Consejo (NIS2) y futuro (transposición la Directiva 2022/2555 del Parlamento Europeo y del Consejo (NIS2) y Ley de Coordinación y

Gobernanza de la Ciberseguridad), y el alineamiento de las propias directrices corporativas con dicha legislación y con las mejores prácticas comúnmente aceptadas internacionalmente en el ámbito de la seguridad de la información (principalmente, todas las distintas normas que componen la serie ISO 27000 de buenas prácticas y gestión de seguridad de la información y el Marco de Ciberseguridad del NIST).

A.2: IDONEIDAD DE LA PROPUESTA PLANTEADA:

Las nuevas amenazas de seguridad surgidas durante los últimos dos años basadas en nuevas técnicas, tácticas y procedimientos de actores de amenazas (*threat actors*) cada vez más preparados, financiados, motivados, e incluso respaldados por gobiernos y estados-nación, así como el creciente uso de la Inteligencia Artificial (IA) como herramienta de ataque, requieren de la actualización y puesta al día de los distintos servicios de seguridad que requiere Canal de Isabel II, S.A. M.P. para afrontarlas, disponiendo para ello de servicios expertos solventes en la prestación de servicios de Centro de Operaciones de Ciberseguridad (SOC) e Inteligencia de Amenazas (*Cyber Threat Intelligence*) desde los puntos de vista táctico, operativo y estratégico (fuentes abiertas (OSINT), Redes Sociales, Foros, Deep Web, Dark Web, etc.), Oficina Técnica de Ciberseguridad (OTS), Gobierno, Gestión del Riesgo, estrategia y cuadros de mando, control y cumplimiento, ciber-resiliencia, cultura de la ciberseguridad empresarial (todo el colectivo de usuarios), revisiones de la seguridad tanto de los servicios ya existentes como de los nuevos servicios y sistemas, auditorías de seguridad internas y externas, medición, gestión y mejora de la eficacia de las acciones de ciberseguridad, evolución del modelo de Detección y Respuesta (EDR) tradicional a las nuevas capacidades de Detección y Respuesta Gestionadas (MxDR), que contemplen el modelado, búsqueda, detección, bloqueo, contención y erradicación de amenazas, investigación en base a hipótesis, la respuesta a incidentes forenses digitales (DFIR), la protección del dato (gobierno y prevención de fugas de información (DLP)), la gestión de la identidad (incluyendo la privilegiada), la monitorización y protección de la infraestructura *on-premise* y *cloud*, etc., la búsqueda proactiva de amenazas (*threat hunting*), la detección de anomalías por análisis de comportamiento (UEBA) y mediante analítica avanzada, etc.

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

La Dirección de Seguridad de Canal de Isabel II, S.A. M.P. no cuenta con todo el personal cualificado necesario para la realización de los trabajos objeto de los Servicios a contratar. Teniendo en cuenta lo anterior, es necesario por tanto externalizar el presente contrato para que se pueda prestar a Canal de Isabel II, S.A. M.P. los Servicios objeto de contratación.

B. JUSTIFICACIÓN DE LOS VALORES ECONÓMICOS

La constante evolución de las amenazas de ciberseguridad, así como el incremento en la complejidad de las Tácticas, Técnicas y Procedimientos (TTPs) utilizados por los actores de amenazas, las nuevas tecnologías emergentes, el mayor uso del *cloud* (SaaS, PaaS e IaaS) como infraestructura crítica corporativa, la implantación de la Inteligencia Artificial en todos los aspectos tecnológicos, la transformación digital y las nuevas regulaciones europeas y nacionales, requieren de una actualización y puesta al día de los distintos servicios de ciberseguridad que ya se prestan a Canal de Isabel II, S.A., M.P. para afrontar dichas amenazas con solvencia, y de la contratación por tanto de

servicios expertos y solventes con capacidad de evolución y adaptación en todos los ámbitos de la ciberseguridad.

Dicha actualización y puesta al día de los distintos servicios de ciberseguridad a prestar a Canal de Isabel II, S.A., M.P. requiere de personal adicional experto dentro de este nuevo contrato con respecto al contrato anterior:

	Recursos mínimos solicitados en PCAP del contrato 5/2021	Total horas 5/2021	Recursos mínimos solicitados en PCAP del contrato 265/2025	Total horas 265/2025
Jefe de Proyecto	1	1.242	3	3.726
Consultor Senior Seguridad	2	3.600	2	7.200
Analista Senior Seguridad	2	3.600	3	10.800
		8.442		21.726

De acuerdo con los objetivos establecidos en el presente contrato objeto de licitación, el equipo de trabajo propuesto deberá estar compuesto, al menos, por los perfiles de ciberseguridad y las horas por año que figuran en la tabla siguiente:

Perfiles de ciberseguridad	Horas / año estimadas por perfil según la dedicación parcial del perfil de Jefe de Proyecto y la dedicación total del resto de perfiles, contemplando una dedicación anual de 1800 horas, tal como se recoge en el XIX Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública	Total horas / año
Jefes de Proyecto (3)	3.726	3.726
Consultores Senior Ciberseguridad (2)	7.200	7.200
Analistas Senior Ciberseguridad (3)	10.800	10.800
		21.726

La estimación de los costes salariales del equipo de trabajo destinado al proyecto, a partir del Anexo I Área 5 (ciberseguridad) del vigente XIX Convenio colectivo estatal de empresas de consultoría (Resolución de 4 de abril de marzo de 2025, de la Dirección General de Empleo, por la que se registra y publica el XIX Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública) y en función de la dedicación de las categorías adscritas a la ejecución del contrato, son los que aparecen en la siguiente tabla:

Coste de personal					
Perfiles	Dedicación	Salario Anual	Coste anual según dedicación	Coste personal contrato	Coste personal contrato con Seguridad Social 30%
Jefe de Proyecto	3.726,00	34.635,37	71.695,22	0	93.203,79
Consultor Senior Seguridad	7.200,00	34.447,56	137.790,24	0	179.127,31
Analista Senior Seguridad	10.800,00	32.346,23	194.077,38	0	252.300,59
	21.726,00				524.631,69

Para la determinación del valor estimado de licitación se han tenido en cuenta los precios de mercado, así como el valor promedio del gasto mensual en los años 2021, 2022, 2023, 2024 y 2025 en el contrato 5/2021 relativo a "SERVICIOS DE CENTRO DE CIBERSEGURIDAD".

Los precios que figuran en los servicios del catálogo de referencia son aquellos incurridos, en promedio, por los distintos departamentos de Ciberseguridad de las compañías consultadas para su prestación, y provienen del análisis e imputación, en general, de la totalidad de las partidas presupuestarias con impacto en los mismos (costes por mantenimientos y servicios internos o externos, seguridad, respaldo, etc.). Dichos precios contemplan los márgenes que dan cobertura a costes estructurales y beneficios empresariales.

Se ha realizado el estudio de los costes de los perfiles a doce (12) meses, usándose un *driver* para la obtención de costes unitarios para servicios básicos de tarifa por hora, lo que se considera a efectos de benchmarking como coste fijo.

Por lo tanto, las tarifas por hora obtenidas para cada uno de los perfiles demandados han sido las que aparecen a continuación:

Tarifas (€/hora) por perfil	Empresa 1	Empresa 2	Empresa 3	Empresa 4
T1 (Jefe de Proyecto)	80,00	49,00	110,00	117,75
T2 (Consultor Senior Seguridad)	60,00	43,55	70,00	74,00
T3 (Analista Senior Seguridad)	40,00	43,55	35,00	60,60

El valor estimado de licitación se ha obtenido multiplicando el total horas de cada perfil por su tarifa media, tal y como se muestra en la siguiente tabla:

Perfiles	Total horas	Tarifa mínima	Tarifa media	Tarifa máxima	Total 1 año	Total 4 años
Jefe de Proyecto	3.726	49,00	83,38	117,75	310.673,88	1.242.695,52
Consultor Senior Seguridad	7.200	43,55	58,78	74,00	423.216,00	1.692.864,00
Analista Senior Seguridad	10.800	35,00	47,80	60,60	516.240,00	2.064.960,00
	21.726				1.250.129,88	5.000.519,52

Se estima, por tanto, un Presupuesto Base de Licitación (PBL) de 5.000.000 € sin IVA porque se considera suficiente para prestar el servicio objeto del contrato y facilita la concurrencia.

El presupuesto base de licitación se corresponde en su totalidad (100%) a los costes de personal tal y como se recoge las tablas anteriores.

El presente contrato supone un incremento del 150% sobre el contrato anterior con número de expediente 5/2021 debido a la mejora y optimización de los procesos de ciberseguridad existentes.

5. PROCEDIMIENTO DE ADJUDICACIÓN

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

RESPONSABLE DEL CONTRATO:

Se designa como responsable del contrato a efectos de lo establecido en el artículo 62 de la LCSP a la jefatura del Área de Ciberseguridad.

Firma/s:

Firmado electronicamente
por MORALES COBOS
OLGA FIRMA

Fdo. P.A. Olga Morales Cobos
Coordinadora Ciberseguridad.
Área Ciberseguridad

Firmado electronicamente
por: RICARDO LLORENTE
HERNÁN-GÓMEZ

Director de Seguridad