MEMORIA JUSTIFICATIVA DE LA CONTRATACIÓN DE LOS SERVICIOS TÉCNICOS DE SOPORTE Y ANÁLISIS PARA SEGURIDAD INTEGRAL EN EL CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y EN LA OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

1.- OBJETO

La presente memoria tiene por objeto justificar la contratación de la prestación de servicios técnicos de soporte y análisis para la seguridad integral en el Gabinete de Coordinación y Estudios, de la Secretaría de Estado de Seguridad (Ministerio del Interior), y en concreto dentro del primer órgano, al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a la Oficina de Coordinación de Ciberseguridad (OCC), focalizados en el análisis en profundidad de las tareas de protección y seguridad para la gestión, seguimiento y resolución de incidentes de seguridad que afecten a Infraestructuras Críticas (IC, de la Ley 8/2011), Operadores de Servicios Esenciales (del RDL 12/2018), operadores estratégicos y sus proveedores; la atención del centro de recepción de incidencias de ciberseguridad gestionada, con soporte 24x7x365; así como apoyo técnico en las labores de persecución de la cibercriminalidad y el ciberterrorismo; y la prestación de un servicio de suministro de información obtenida a través de distintas fuentes, que permita a los analistas de la OCC y del CNPIC evaluarla oportunamente con objeto de desarrollar los cometidos que tiene encomendados, entre los que se encuentran la monitorización y la vigilancia digital en busca de ciberamenazas de distinta naturaleza relacionadas con el terrorismo y ciberterrorismo, hacktivismo, movimientos radicales, cibercriminalidad y ciberataques o acciones cibernéticas llevadas a cabo por otros Estados y que puedan tener impacto sobre intereses españoles materializados en los operadores referidos, para proveer informes estratégicos y operativos a las altas instancias del Ministerio del Interior, Secretaría de Estado de Seguridad, Dirección General de la Policía y Dirección General de la Guardia Civil.

La contratación no se estructura en lotes, puesto que la realización independiente de las diversas prestaciones dificultaría la correcta ejecución del servicio, por la propia naturaleza del objeto de este contrato con autonomía propia que conlleva tener un conocimiento global de las tareas inherentes al mismo bajo una única dirección de proyecto, lo que implica la necesidad de coordinar la ejecución de las prestaciones, que podrían verse imposibilitadas por su división en lotes.

2.- NECESIDAD E IDONEIDAD

El Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, asigna al Gabinete de Coordinación y Estudios impulsar, coordinar y supervisar, a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), todas las actividades que tiene encomendadas la Secretaría de Estado en relación con la protección de las infraestructuras críticas en el

territorio nacional, en colaboración con otros Departamentos ministeriales.

Por otra parte, en el ámbito de la ciberseguridad, la legislación vigente encomienda a la Oficina de Coordinación de Ciberseguridad (OCC), del Gabinete de Coordinación y Estudios, de la Secretaría de Estado de Seguridad (Ministerio del Interior), un papel relevante en la gestión de los ciberataques a los sistemas de información de los Operadores Críticos, de Servicios Esenciales y otros estratégicos y sus proveedores, así como en la coordinación técnica de las actividades operativas y de investigación que, en ese ámbito, requieren la implicación de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado.

En este sentido, la OCC asume las competencias de coordinación técnica del Ministerio del Interior con el INCIBE-CERT en la gestión y resolución de incidentes en materia de ciberseguridad, sin perjuicio de otras acciones llevadas a cabo en conjunción con el CCN-CERT del Centro Nacional de Inteligencia y otros CSIRT nacionales.

Además, el Real Decreto 734/2020, establecen que la OCC actúa como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

Por otro lado, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, asigna, al mismo tiempo, a la Secretaría de Estado de Seguridad, importantes responsabilidades en la gestión y comunicación de incidentes de seguridad sufridos por los operadores de servicios esenciales.

El crecimiento en el número de incidentes de ciberseguridad con impacto en los Operadores Críticos y en los de Servicios Esenciales así como en otros considerados estratégicos nacionales; el aumento de las tipologías de ciberataque, su evolución y complejidad; así como el aumento en el número de requerimientos recibidos en la OCC por parte de los Operadores y otras entidades gubernamentales para la resolución y esclarecimiento de los incidentes de seguridad de los sistemas de información de una forma conjunta y coordinada, han requerido el desarrollo de una serie de capacidades que, si bien en algunos casos se han venido prestando de forma exclusiva desde la OCC, han sido objeto de una potenciación y continuidad estable en el tiempo, que ha permitido operar las 24 horas del día, los 7 días de la semana, 365 días al año con una calidad en el servicio acorde con la importancia en la protección de infraestructuras críticas. La gestión de estos incidentes exige especialización, disponibilidad y respuesta inmediata en tanto en cuanto podrían llegar a afectar a los servicios esenciales prestados por Operadores Críticos nacionales y Operadores estratégicos y sus proveedores.

Teniendo en cuenta las necesidades planteadas, se considera idónea la contratación de un servicio que permita dar continuidad al soporte actual que está recibiendo el

centro de atención de incidencias de ciberseguridad de la OCC, disponiendo de manera estable y continua durante las 24 horas del día, los 7 días de la semana, un servicio que permite la gestión de herramientas de tipo complejo y con capacidad de análisis sobre incidentes, debido a que se trata de actividades que requieren que en ese servicio se aúne las exigencias de alta especialización, disponibilidad y respuesta inmediata, y que, actualmente, no puede prestarse directamente por el CNPIC y la OCC, ni por las Direcciones Generales de la Policía y Guardia Civil, al carecer de las capacidades descritas para el tratamiento y la gestión de la Ciberseguridad.

3.- CONTENIDO DE LAS PRESTACIONES DEL CONTRATO

Las prestaciones objeto de contratación serán las siguientes:

3.1. Para los servicios de soporte de atención de incidencias de ciberseguridad (24x7x365):

- Gestión integral de incidentes de ciberseguridad y seguridad física.
- Operación y gestión del sistema de comunicación AlertPIC.
- Atención del punto de contacto nacional para el intercambio de información en las peticiones de ayuda policial por parte de otros estados miembros conforme lo establecido en la Directiva 2013/40 y legislación adoptada por la Secretaría de Estado de Seguridad.

3.2. Para los servicios de apoyo técnico para el análisis en profundidad de las tareas de protección y seguridad para la gestión, seguimiento y resolución e incidentes.

El análisis en profundidad de las tareas de protección y seguridad de la información de Infraestructuras Críticas, Operadores de Servicios Esenciales, operadores estratégicos y sus proveedores, para la gestión, seguimiento y resolución de incidencias comporta la realización de las siguientes tareas:

- Realización de tareas de consultoría en materia de ciberseguridad
- Realización de tareas de detección de incidentes de ciberseguridad
- Realización de tareas de reacción ante incidentes de ciberseguridad
- Realización de tareas de análisis de patrones y tendencias de los incidentes de ciberseguridad
- Elaboración de informes estadísticos en materia de ciberseguridad.
- Gestión de activos tecnológicos
- Realización de labores de cibervigilancia (vigilancia digital y tecnológica) en redes sociales u otros entornos y redes digitales o virtuales, empleando herramientas que faciliten las labores de ciberinteligencia y monitorización del ciberespacio.
- Supervisión y coordinación con la actividad del servicio de provisión de información.

3.3. Para los servicios de provisión de información

Suministro a la OCC y al CNPIC de información sobre las materias y mediante los entregables que se describen en el Pliego de Prescripciones Técnicas:

- Sobre yihadismo.
- Sobre hacktivismo.
- Sobre cibercriminalidad.
- Sobre acciones atribuibles a otros Estados.
- Sobre acciones atribuibles a movimientos radicales.
- Sobre eventos de especial interés.

4.- DURACIÓN DEL CONTRATO

De cara a garantizar la continuidad de los servicios descritos en el presente documento, además de consolidar el seguimiento de los procedimientos internos del Gabinete de Coordinación y Estudios, se hace necesario establecer la duración del contrato en 24 meses, a contar desde el 1 de junio de 2021 o desde el día siguiente al de la formalización del contrato, en caso de fuese posterior, y podrá prorrogarse una o más veces al vencimiento del plazo de vigencia señalado o de sus prórrogas, siendo las que se acuerden obligatorias para el adjudicatario previo aviso mínimo de dos meses.

La prórroga, así acordada, no podrá tener una duración superior a veinticuatro (24) meses y, en ningún caso, la duración total del contrato, incluidas las prórrogas, podrá superar los cuarenta y ocho (48) meses.

5.- PRESUPUESTOS Y APLICACIÓN PRESUPUESTARIA. ANUALIDADES.

5.1 Valor estimado del contrato

El valor estimado del contrato se ha calculado mediante la suma de las siguientes cantidades:

- El importe del presupuesto de licitación sin IVA por VEINTICUATRO MESES.
- El importe del presupuesto de licitación sin IVA por VEINTICUATRO MESES de prórroga.

De acuerdo con ello, el desglose del valor estimado del contrato es el que se recoge en el siguiente cuadro:

	Importe	**Prórroga**	**Total**
Valor estimado	1.298.932,86	1.298.932,86	2.597.865,72

5.2 Presupuesto base de licitación

El Presupuesto base de licitación asciende a 1.298.932,86 euros. Dicho importe se verá incrementado en el correspondiente al Impuesto sobre el Valor Añadido (IVA) que se eleva a 272.775,90 euros, arrojando un importe total de 1.571.708,76 euros.

La distribución del presupuesto es la que se recoge en el siguiente cuadro:

Costes directos (Salarios y costes sociales)	
Salarios	862.072,66
Costes sociales	241.377,06
Total costes directos	**1.103.449,72**
Costes indirectos	
Gastos generales	77.400,00
Beneficio industrial	118.083,14
Total costes indirectos	**195.483,14**
TOTAL ESTIMACIÓN COSTES	**1.298.932,86**

Para su elaboración se ha tenido en cuenta los costes de mano de obra de la licitación del contrato que actualmente está en ejecución para los servicios de apoyo técnico al Centro Nacional de Protección de infraestructuras y Ciberseguridad (Exp. 18P1200). También se ha considerado el XVII Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública, tomando como referencia el grupo B2 para los analistas y el grupo D1 para los operadores.

Costes directos

- Salarios.
- Costes sociales.

Costes indirectos

- Gastos generales.
- Beneficio industrial.

Los costes directos son los derivados de la intervención en el contrato del personal necesario para la ejecución de las prestaciones correspondientes, cuyo dimensionado y dedicación deberán ser establecidos por la empresa adjudicataria, teniendo en cuenta la adscripción de medios mínima establecida en el Pliego de Prescripciones Técnicas, sin perjuicio del nombramiento de un Coordinador Técnico o Punto de Contacto (PoC).

Los gastos generales se refieren a los que se deriven de la puesta a disposición de los medios humanos y materiales adscritos, con sus correspondientes medios ofimáticos, que el adjudicatario precise para la gestión del contrato (gestión del personal, elaboración y tramitación de nóminas, emisión y tramitación de la facturación, emisión, procesamiento y control de partes de trabajo, informes de gestión, entregables); teniendo en cuenta el volumen de personal a adscribir y los trabajos a realizar se han estimado tomando como referencia los derivados de la ejecución del citado contrato 18P1200.

El beneficio industrial se ha estimado, teniendo en cuenta el montante del contrato, el tiempo de ejecución y la especificidad de los servicios a realizar, en un 10 % de los costes directos y de los gastos generales.

5.3 Aplicación presupuestaria

El gasto se financiará con cargo al presupuesto vigente de la Secretaría de Estado de Seguridad, aplicación presupuestaria **16.02.132A.227.06**.

5.4 Sistema de fijación del precio y pagos al contratista

El precio del contrato es a tanto alzado, facturándose los servicios de forma lineal, a mes vencido.

En consecuencia, la facturación de los meses de diciembre de cada una de las anualidades se presentará en el mes de enero de la siguiente anualidad.

Anualidades de gasto

De acuerdo con el sistema de pagos previsto, la distribución del gasto, incluido el IVA, por anualidades es la que se indica a continuación:

Anualidad 2021 (€)	**Anualidad 2022 (€)**	**Anualidad 2023 (€)**
392.927,19	785.854,38	392.927,19

6.- CLASIFICACIÓN Y CRITERIOS DE SOLVENCIA.

6.1. Clasificación.

Conforme al artículo 77.1. b) de la LCSP no se exige la clasificación del empresario, por tratarse de un contrato de servicios, no figurando el Código del Vocabulario Común de Contratos Públicos (CPV) asignado a este contrato en el anexo II del Reglamento General de la Ley de Contratos de las Administraciones Públicas aprobado por RD 1089/2001, de 12 de octubre.

El licitador podrá acreditar su solvencia acreditando el cumplimiento de los requisitos recogidos en el Cuadro del PCAP que regirá este expediente.

6.2. Justificación de los Criterios de solvencia seleccionados.

El presente contrato de servicios no ofrece una especial complejidad para su ejecución por cuanto que, salvo que para asegurar un adecuado nivel en los trabajos se ha establecido la necesidad de adscribir a la ejecución del contrato un equipo mínimo de profesionales con un perfil profesional adecuado a la naturaleza de las prestaciones que comporta.

Se considera por ello que el criterio más relevante para acreditar la **solvencia económica y financiera** es el referido al volumen anual de negocios que debe ser suficiente para colegir que las licitadoras tienen potencial económico y financiero para el cumplimiento del contrato.

En este sentido, y con el fin de no limitar la concurrencia, se considera suficiente la aplicación del criterio general establecido en el artículo 87.1.a) de la LCSP, y por ello, se ha recogido en los pliegos que la solvencia económica y financiera se acreditará mediante el volumen anual de negocios del licitador que referido al año de mayor volumen de negocio de los tres últimos concluidos deberá ser equivalente a una vez el valor estimado del contrato sin IVA y sumando la prórroga, y que se concreta en un importe de 2.597.865,72 € de euros.

Por las mismas razones, se considera que los criterios de acreditación de la **solvencia técnica** deben basarse fundamentalmente en la experiencia en la realización de servicios realizados de análoga naturaleza, complementados en este caso con la gestión de la calidad en los procesos internos de las empresas licitadoras.

En relación con la experiencia en la realización de servicios realizados de análoga naturaleza, y con el fin de no limitar la concurrencia, se considera suficiente la aplicación del criterio general establecido en el artículo 90.1.a) de la LCSP, así como en el Reglamento General de la Ley de Contratos de las Administraciones Públicas, consistente en la acreditación de una relación de los principales servicios o trabajos efectuados durante los últimos tres años correspondientes al mismo o similar tipo o naturaleza que los que constituyen el objeto del contrato. El requisito mínimo será que el importe anual acumulado en el año de mayor ejecución sea igual o superior al 70%

del valor estimado del contrato: 909.253 €.

7.- PROCEDIMIENTO DE ADJUDICACIÓN

Se propone la adjudicación del contrato **por el procedimiento abierto**, que es el procedimiento ordinario de adjudicación de los contratos públicos, al no concurrir circunstancias específicas que hagan conveniente la utilización de un procedimiento distinto.

En razón a la cuantía del valor estimado del contrato, tendrá la consideración de contrato sometido a regulación armonizada.

8.- CRITERIOS DE ADJUDICACIÓN DEL CONTRATO

Los criterios para la adjudicación del contrato – recogidos en el Cuadro de Características del Pliego de Cláusulas Administrativas Particulares de este Contrato – se centran en:

8.1. El Precio, al que se otorga un peso específico del 51% sobre la valoración total de las ofertas; a la oferta más económica se le asignarán **51 puntos**. Las restantes ofertas serán puntuadas con criterios de proporcionalidad.

8.2. La **adscripción al servicio de licencias adicionales a las requeridas como mínimos en los puntos 4.2.1 y 4.2.2 del PPT**. El incremento de UN bloque adicional de 4 licencias, compuesto por 1 TABLEAU versión creator o similar, 1 SHODAN o similar, 1 NESSUS o similar y 1 DOMAIN TOOLS o similar, se valorará con 3 puntos, hasta un **máximo de CUATRO bloques (12 puntos)**.

8.3. La **mejora del perfil profesional de coordinador y analistas** de ciberseguridad que se describen en el apartado 7.1 del PPT. Por cada año de experiencia profesional de todos los perfiles (coordinador y analistas) se otorgarán **3 puntos** hasta un **máximo de 12 puntos**.

8.4. La **mejora del perfil profesional de coordinador y analistas** de ciberseguridad que se describe en el apartado 7.1 del PPT. Según los requisitos a valorar recogidos en los apartados A) y B):

A) Encontrarse en posesión de Máster Universitario en materia de ciberseguridad
B) Disponer de certificaciones en la materia. CEH/OSCP/CISA/CISM/CISSP

al que se le otorgará un peso del **1 punto** por cada perfil que acredite A) o B), hasta un **máximo de 5 puntos.**

8.5. El **incremento de UN analista tipo 1 y UN analista tipo 2** a disposición del

contrato sobre el mínimo establecido en el apartado 7.1 del PPT, en la modalidad de presencia de lunes a viernes en las instalaciones del CNPIC, al que se le otorgará un peso de **9 puntos para el analista tipo 1** y otros **9 puntos para el analista tipo 2**, hasta un **máximo de 18 puntos**.

8.6. El **incremento en el número de servicios de provisión de información sobre eventos de especial interés** del apartado 3.3.6 del PPT, al que se le otorgará **UN punto por cada servicio**, hasta un **máximo** de **DOS servicios** (**2 puntos**).

Justificación:

Se ha decidido establecer un sistema puramente objetivo sin dar margen a la subjetividad, garantizando de esta forma una total y absoluta transparencia en la designación del adjudicatario.

El precio es, a efectos de adjudicación, el criterio más importante y de mayor relevancia y por ello se ha otorgado al mismo un peso específico del 51 por 100.

Junto al criterio relativo al precio se han establecido otros cinco criterios objetivos que permiten reforzar algunas de las prestaciones del contrato que se consideran de interés para la Administración, teniendo en cuenta que su inclusión en la oferta tiene un peso importante en el sentido de que, si bien cada uno de ellos y por sí solo no es decisivo para la adjudicación del contrato, influyen de manera efectiva en el resultado final, en función de su inclusión o no en la misma:

Por una parte, el incremento del número de analistas, sin coste para la Administración, cumple una finalidad muy importante de cara a complementar adecuadamente algunas de las tareas tasadas en el PPT, permitiendo acometer situaciones de carácter extraordinario o imprevisible y viene a reforzar las prestaciones del contrato en interés de la Administración.

Por otra parte, con carácter general el PPT establece unos requisitos específicos de perfiles profesionales, tanto de coordinador como de analista. Se considera que la mejora en ambos requisitos mínimos contribuiría a mejorar ostensiblemente la calidad del servicio a prestar, repercutiendo al mismo tiempo en la mejora de la imagen institucional y labores del Gabinete de Coordinación y Estudios en materia de Ciberseguridad y Cibercriminalidad a nivel nacional e internacional.

9.- PRESENTACIÓN DE OFERTAS.

Para la presente contratación, en la presentación de ofertas se exigirá el empleo de medios electrónicos, conforme a lo dispuesto con carácter general en la LCSP, en los términos que recogerá el Cuadro del PCAP.

10.- TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Las actuaciones que se produzcan como consecuencia del desarrollo de este contrato se ajustarán en todo caso a lo establecido en la normativa vigente acorde o derivada de la trasposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, la normativa de secretos oficiales y materias clasificadas; y, en lo que le sea de aplicación, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y demás normativa de desarrollo.

En consecuencia, asimismo, al requerir la ejecución del contrato el tratamiento de datos de carácter personal, resultan de aplicación las previsiones establecidas en la Disposición adicional vigésima quinta de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

El tratamiento de datos personales que se derivará para la consecución del objeto del presente contrato es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, tal y como establece el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, así como el resto denla legislación vigente en la materia.

La información sólo podrá utilizarse para el cumplimiento de las funciones legalmente encomendadas o su incorporación al procedimiento administrativo del que traen su causa, solo pudiendo ser objeto de comunicación a aquellos terceros que se especifiquen y en función del cumplimiento de las citadas funciones. En ningún caso, participarán en el intercambio de información a órganos o personas distintas de las designadas como competentes.

La violación de estas obligaciones conllevará la exigencia por la autoridad competente de las responsabilidades penales, administrativas y civiles a que diera lugar.

Para el cumplimiento del objeto del presente contrato el Ministerio del Interior y la empresa adjudicataria deberán tratar los datos personales de los cuales la Secretaría de Estado de Seguridad es responsable del tratamiento, de la manera que se especifique en contrato de encargado de tratamiento, firmado por ambas partes, como máximo dentro de los 15 días siguientes a la formalización del contrato principal. En

dicho contrato se describirá, en detalle, los datos personales a proteger, así como el tratamiento a realizar y las medidas a implementar por la empresa adjudicataria, como encargo de tratamiento.

Ello conlleva que la empresa adjudicataria actúe en calidad de encargado del tratamiento y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los datos personales.

Por tanto, sobre la Secretaría de Estado de Seguridad recaen las responsabilidades del responsable del tratamiento y sobre la empresa adjudicataria las de encargado de tratamiento. Si éste último destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del presente convenio y/o la normativa vigente, será considerado también como responsable del tratamiento, respondiendo de las infracciones en que hubiera podido incurrir.

Madrid, 19 de noviembre de 2020

El Director del Gabinete de Coordinación y Estudios

Fdo.: José Antonio Rodríguez González