MEMORIA JUSTIFICATIVA DE LA CONTRATACIÓN DE LOS SERVICIOS TÉCNICOS DE SOPORTE DE CIBERSEGURIDAD GESTIONADA Y DE ANÁLISIS EN PROFUNDIDAD DE LAS TAREAS DE PROTECCIÓN Y SEGURIDAD PARA LA GESTIÓN, SEGUIMIENTO Y RESOLUCIÓN DE INCIDENTES DE CIBERSEGURIDAD Y CIBERTERRORISMO.

1.- OBJETO

La presente memoria tiene por objeto justificar la contratación de servicios de apoyo técnico al Centro Nacional de Protección de infraestructuras y Ciberseguridad –CNPIC- para 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, para 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 ciberdelincuencia y el ciberterrorismo.

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 Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio de Interior, es el órgano encargado de la dirección y coordinación de las actividades derivadas de la protección de las Infraestructuras Críticas, además de ser Autoridad Competente para los Operadores de Servicios Esenciales.

En el ámbito de la ciberseguridad, la legislación vigente asigna a la Oficina de Coordinación Cibernética –OCC- de dicho Centro 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 (FFCCSE).

La Instrucción de la Secretaría de Estado de Seguridad 15/2014 y el Real Decreto 952/2018, asignan a la OCC las competencias de coordinación técnica del Ministerio del Interior con el anteriormente conocido como CERT de Seguridad e Industria (CERTSI), hoy 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 la Instrucción 2/2016 de la Secretaría de Estado de Seguridad, y el Real Decreto 952/2018 establecen la OCC como punto de contacto nacional para el intercambio de información con la Comisión Europea y con los Estados miembros en relación a los ataques contra los sistemas de información, conforme a lo establecido en el artículo 8 de la Directiva 2013/40/UE, 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 también a la OCC 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, requieren el desarrollo de una serie de capacidades, que si bien en algunos casos se han venido prestando de forma exclusiva desde la OCC, requieren de una potenciación y continuidad estable en el tiempo, que permita 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.

Por otra parte, la inminente implantación del sistema AlertPIC permitirá la comunicación entre el CNPIC y los operadores de forma confidencial y permanente en el tiempo, con una dependencia tecnológica exclusiva en sistemas propietarios y desarrollados por el Ministerio del Interior con una disponibilidad 24x7x365. La logística necesaria para la puesta en producción de este sistema de comunicación requiere de una operativa 24x7x365, con un soporte continuo de incidencias y ante interrupciones en el servicio.

Teniendo en cuenta las necesidades planteadas, se considera idónea la contratación de un servicio que permita dar soporte al centro de atención de incidencias de ciberseguridad, con una implantación estable y continua durante las 24 horas del día, los 7 días de la semana, gestionando herramientas de tipo complejo (como la ya mencionada AlertPIC) y con capacidad de análisis sobre dichos incidentes, actividades que requieren que en ese servicio se aúne las exigencias de alta especialización, disponibilidad y respuesta inmediata, servicio que actualmente no puede prestarse

directamente por el CNPIC, 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):

- Resolución de incidentes de ciberseguridad clasificados como de NIVEL 1, y de operación y escalado de aquellos otros que sean considerados de NIVEL 2 de operación
- 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.

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 auditorías de Ciberseguridad.
- Monitorización y vigilancia digital de activos tecnológicos.
- Consulta a Interfaces de Programación de Aplicaciones de Redes Sociales (RR.SS), y uso de cualquier otra aplicación que facilite las labores de Ciberinteligencia y monitorización del ciberespacio
- Mitigación, investigación y resolución de incidentes cibernéticos, en los que medie malware, amenazas avanzadas persistentes.

4.- DURACIÓN DEL CONTRATO

El plazo total del contrato es de 12 meses a partir del día 1 de abril de 2019 o a partir del 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 doce (12) meses y, en ningún caso, la duración total del contrato, incluidas las prórrogas, podrá superar los veinticuatro (24) 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
- El importe del presupuesto de licitación sin IVA de DOCE 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	432.726,00	432.726,00	865.452,00

5.2 Presupuesto base de licitación

El Presupuesto base de licitación asciende a 432.726,00 euros. Dicho importe se verá incrementado en el correspondiente al Impuesto sobre el Valor Añadido (IVA) que se eleva a 90.872,46 euros, arrojando un importe total de 523.598,46 euros.

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

Costes directos (Salarios y costes sociales)	
Salarios	293.273,00
Costes sociales	82.115,00
Total costes directos	**375.388,00**
Costes indirectos	
Gastos generales	18.000,00
Beneficio	39.338,00
Total costes indirectos	**57.338,00**
TOTAL ESTIMACIÓN COSTES	**432.726,00**

Para su elaboración se ha tenido en cuenta los costes de mano de obra, derivados de los datos de los precios medios por hora más frecuentes en los pliegos de soporte y mantenimiento de sistemas similares al actual, donde no consta que existan diferencias por razón de género; 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, 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, gastos de las inspecciones de Ciberseguridad , etc.); teniendo en cuenta el volumen de personal a adscribir y los trabajos a realizar se han estimado en 1.500 euros/mes, es decir, 18.000 euros.

El beneficio 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, a razón de una duodécima parte del precio de adjudicación cada mes.

En consecuencia, la facturación del mes de diciembre de 2019 se presentará en el mes de enero de 2020.

Con arreglo a ello, en el año 2019 se facturarán 8 meses y en año 2020 cuatro meses.

5.5 Anualidades de gasto

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

Anualidad 2019 (€)	Anualidad 2020 (€)
349.065,64	174.532,82

6.- CLASIFICACIÓN Y CRITERIOS DE SOLVENCIA.

6.1. Clasificación.

No se exige clasificación por no figurar 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 y media el valor estimado del contrato y que se concreta en un importe de 1.298.178,00 €. 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 89.1.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: 605.816,40 euros.

Estos criterios son los establecidos con carácter general en el Reglamento General de la Ley de Contratos de las Administraciones Públicas.

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.

No obstante lo anterior, concurren en el presente expediente de contratación razones que hacen necesaria la declaración de urgencia del expediente de contratación, que tienen encaje en los presupuestos del artículo 119 de la LCSP.

En el ámbito de la ciberseguridad, el Real Decreto 925/2018, de 27 de julio, de reorganización del Ministerio del Interior, asignó a la Oficina de Coordinación Cibernética (OCC) del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio de Interior, un papel relevante en la gestión de la prevención y lucha contra los ciberataques a los sistemas de información de los operadores críticos, así como en la coordinación técnica de las actividades operativas y de investigación que, en este ámbito, requieren la implicación de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado.

Esta función de coordinación se potenció con la aprobación del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, para la transposición de 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, y asigna a la Secretaría de Estado de Seguridad, a través del CNPIC el papel de autoridad para una serie de operadores de servicios esenciales que no bajan de 200. El cumplimiento de estas funciones encomendadas, que deberían ponerse en marcha de manera inmediata, requieren obligatoriamente la existencia de capacidades 24x7 en materia de Ciberseguridad.

Por otra parte, otra de las funciones que ejerce la OCC del CNPIC es la de establecerse como punto de contacto nacional de coordinación operativa 24x7 para el

intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo dispuesto por la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra sistemas de información. Como consecuencia de esta directiva, se transpusieron una serie de tipos penales de nuevo cuño y se readaptaron otros que ya se introdujeron en nuestro Código Penal, a través de la L.O. 1/2015.

Conforme al artículo 13 de la mencionada Directiva, "*a través del intercambio de información sobre las infraestructuras mencionadas en los artículos 3 al 8, los Estados miembros garantizarán que tienen un punto de contacto nacional operativo y harán uso de la red existente de puntos de contacto operativos disponibles veinticuatro horas al día, siete días a la semana. Los Estados miembros también asegurarán de que cuentan con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda si la misma será atendida, y la forma y el plazo aproximado en que lo será*".

El artículo 119 de la vigente Ley de Contratos del Sector Público establece que podrán ser objeto de tramitación urgente –con las especialidades contempladas en el mismo- los expedientes correspondientes a los contratos cuya celebración responda a una necesidad inaplazable o cuya adjudicación sea preciso acelerar por razones de interés público.

En el presente caso la celebración del contrato se enmarca en la necesidad de comenzar de forma inmediata la ejecución de la función de coordinación respecto a la gestión y comunicación de incidentes de seguridad sufridos por los operadores de servicios esenciales, encomendada en el Real Decreto-ley 12/2018 y que requieren obligatoriamente la existencia de capacidades 24x7 en materia de Ciberseguridad, así como en la necesidad de cumplir con lo dispuesto por la Directiva 2013/40/UE, habilitando las capacidades de punto de contacto nacional operativo, y al mismo tiempo evita incumplimientos por parte de España en materia de ciberseguridad. Existen por ello razones de interés público y necesidad inaplazable que aconsejan acelerar la celebración del contrato.

El procedimiento ordinario requiere unos plazos de tramitación estimados que, en conjunto, pueden ser superiores a seis meses, plazo de tiempo que es preciso reducir lo máximo posible. Por dicha razón, se considera necesario declarar de urgencia la tramitación del presente expediente de contratación, que permita aplicar las especialidades contempladas en el artículo 119.2 de la LCSP, ya citado.

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 49% sobre la valoración total de las ofertas; a la oferta más económica se le asignarán 49 puntos. Las restantes

ofertas serán puntuadas con criterios de proporcionalidad.

8.2. El incremento del número de inspecciones en instalaciones para la realización de auditorías de ciberseguridad, sobre el mínimo establecido en el apartado 4.2.1. del PPT, al que se le otorgará un peso del 18%; a cada empresa licitadora se le otorgará la puntuación directa que obtenga en la valoración de este criterio, hasta el límite máximo establecido de 18 puntos.

8.3. La mejora del perfil profesional de los operadores que se describe en el apartado 6.1 del PPT, con respecto de los años de experiencia profesional, al que se le otorgará un peso del 15%; a cada empresa licitadora se le otorgará la puntuación que obtenga en la valoración de este criterio, hasta el límite máximo establecido de 15 puntos.

8.4. La mejora del perfil profesional de los analistas de ciberseguridad que se describe en el apartado 6.1 del PPT, no sólo respecto de los años de experiencia profesional, sino también respecto de la habilitación de Seguridad NATO y/o EU, al que se le otorgará un peso del 8%; a cada empresa licitadora se le otorgará la puntuación que obtenga en la valoración de este criterio, hasta el límite máximo establecido de 8 puntos.

8.5. El incremento de UN analista a disposición del contrato sobre el mínimo establecido en el apartado 6.1 del PPT, en la modalidad de presencia de lunes a viernes en las instalaciones del CNPIC, al que se le otorgará un peso del 10%; a cada empresa licitadora se le otorgará la puntuación que obtenga en la valoración de este criterio, hasta el límite máximo establecido de 10 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 de los cinco, por lo que se le otorga un peso específico del 49 por 100.

Junto al criterio relativo al precio se han establecido otros 4 criterios objetivos que permiten reforzar, con un peso total del 51 por 100, 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 muy importante en el sentido de que, si bien cada uno de ellos y por sí solo no es decisivo para la adjudicación del contrato, sí que 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 inspecciones y 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 operador 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 CNPIC en materia de Ciberseguridad 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

La ejecución de las prestaciones del contrato no implica el manejo de datos de carácter personal.

En consecuencia, no resultan de aplicación las previsiones establecidas en la disposición adicional vigesimoquinta de la LCSP.

Madrid, 23 de noviembre de 2018

El Director del Centro Nacional de Infraestructuras y Ciberseguridad.

Fernando J. Sánchez Gómez