Memoria justificativa de expediente de contratación

Revisados los informes de la Asesoría Jurídica de fecha 4 de octubre de 2024 y 16 de octubre de 2024 relativos a este contrato, se tramita esta nueva memoria con objeto de solventar las distintas cuestiones planteadas en dichos informes.

1. DENOMINACIÓN DEL CONTRATO

SUMINISTRO DE UNA SOLUCIÓN DE DOBLE BARRERA DE FIREWALL DE PERÍMETRO EN EL CPD.

2. OBJETO

El objeto de este contrato es el suministro de los elementos necesarios para contar con una solución de doble nivel de firewall de perímetro, la cual es necesaria para garantizar un adecuado nivel de seguridad en el Centro de Proceso de Datos principal y secundario del Gobierno de Cantabria.

Actualmente el Gobierno de Cantabria cuenta con una plataforma de firewalls del fabricante Fortinet en el primer nivel de firewall de perímetro del Centro de Proceso de Datos (CPD) principal, es por esto que en la segunda barrera de firewall de perímetro se requiere de un fabricante diferente para tener diferentes fortalezas en todas las características de seguridad implementadas. Este contrato permitirá equipar tanto las instalaciones del CPD principal como del CPD secundario de este equipamiento de seguridad para una mejora drástica de la defensa perimetral ante ataques externos

Para determinar la naturaleza de este contrato (contrato de suministro) se atenderá a la calificación que indica el artículo 16.3. b) de la LCSP en los que considera contratos de suministro “Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información”

3. JUSTIFICACIÓN DEL OBJETO

La modernización de la Administración de la Comunidad Autónoma de Cantabria es un objetivo prioritario en su propósito de ofrecer a los ciudadanos unos servicios de alta calidad basados en parámetros de eficacia y eficiencia. Para lograr este objetivo es necesario contar con centros de proceso de datos protegidos adecuadamente por diversas capas de defensa antes los ataques cibernéticos.

Por lo tanto, la ciberseguridad es una prioridad dentro los proyectos de la Administración de la Comunidad Autónoma de Cantabria, ya que las amenazas y los ataques son cada vez más sofisticados y con más impacto en los servicios públicos. Una forma destacada y eficaz de aumentar la seguridad es implementar dos niveles de firewall de distintos fabricantes. De esta manera se consigue aumentar considerablemente la protección en las redes y en los activos críticos ante las ciberamenazas en constante evolución.

El Gobierno de Cantabria cuenta actualmente con una plataforma de firewalls del fabricante Fortinet en el primer nivel de firewall de perímetro del Centro de Proceso de Datos. Es por esto que en la segunda barrera de firewall de perímetro se requiere un fabricante diferente para tener diferentes fortalezas en todas las características de seguridad implementadas. Este contrato permitirá equipar tanto en el CPD principal como en el CPD secundario de este equipamiento de seguridad para una mejora decisiva de la defensa perimetral.

Este suministro para las instalaciones del Centro de Proceso de Datos proporciona la seguridad y disponibilidad adecuada para toda la red corporativa y para todos los sistemas alojados en él. Este suministro permite al Centro de Proceso de Datos de la Dirección General de Informática prestar los servicios asociados a todas las aplicaciones del Gobierno de Cantabria en las debidas condiciones de calidad y seguridad. También permite proteger a todos los servicios esenciales de la Administración de la Comunidad Autónoma.

Igualmente garantizar todos los aspectos asociados a la seguridad informática de los sistemas corporativos es vital para la correcta prestación de los servicios públicos ofrecidos por el personal del Gobierno de Cantabria. Este suministro permite a la Administración de la Comunidad Autónoma de Cantabria cumplir con las medidas de seguridad que establece el Esquema Nacional de Seguridad, ya que permite aplicar todas las actualizaciones y parches de seguridad de los productos incluidos en el contrato.

Implementando dos niveles de firewall de distintos fabricantes se consigue una arquitectura de defensa en profundidad que proporciona las siguientes ventajas.:

- Seguridad diversificada: Reduce el riesgo de vulnerabilidades comunes mejorando la seguridad en general. Cada firewall puede detectar y bloquear diferentes tipos de ataques, lo que reduce la posibilidad de que un ataque tenga éxito.
- Reducción de la superficie de ataque: Al dividir las tareas de seguridad entre dos firewalls, se reduce la superficie de ataque que los ciberdelincuentes pueden explotar.
- Redundancia y resiliencia: En caso de fallo de un fabricante, el otro firewall puede mantener la seguridad de la red, proporcionando una capa adicional de resiliencia.
- Mejora en la detección de amenazas: Diferentes fabricantes pueden tener diferentes enfoques y algoritmos distintos para la detección de amenazas

La utilización de dos niveles de cortafuegos, en cascada y de dos fabricantes diferentes, está orientada al cumplimiento del “Artículo 9. Existencia de líneas de defensa” del “Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad”. Esta doble línea aumenta la resistencia ante ciberataques de penetración o de bloqueo de sistemas e incrementa la capacidad de recuperación ante eventuales perturbaciones. Todo ello con la finalidad de mejorar en nuestra Administración las garantías de seguridad de los servicios electrónicos a los que alude el “Capítulo V” de la “Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público”.

4. LOTES

Lote único → Prestación del suministro de forma integral

En lo relativo a la licitación de forma independiente de cada una de las partes de este contrato, no se considera viable su división en lotes debido a la naturaleza del mismo. Esta licitación comprende una unidad funcional de productos, siendo necesaria una recepción coordinada de los mismos en tanto a que nos encontramos con un conjunto de elementos asociados a una misma funcionalidad (suministro de una solución de segunda barrera firewall de perímetro para el Centro Proceso de Datos) que deben ser recibidos de una forma única.

Cabe indicar que la licitación independiente de cada uno de los elementos (hardware o licencias software) asociadas al sistema de seguridad imposibilitaría la puesta en servicio integral de los mismos. Una recepción parcial, tanto individualmente de los sistemas de seguridad como de sus licencias, conllevaría la imposibilidad técnica de realizar un despliegue completo y funcional del sistema de seguridad.

5. ASPECTOS RELACIONADOS CON EL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

Este contrato se cofinanciará con los fondos asociados a la inversión 3 del componente 11 del Plan de Recuperación, Transformación y Resiliencia dentro del marco del Mecanismo de Recuperación y Resiliencia del Ministerio de Hacienda y Función Pública para la transformación digital y modernización de las comunidades autónomas. En concreto este contrato está asociado al proyecto denominado “Mejora de la ciberseguridad a través de la implantación de un 2º nivel de firewall corporativo”, proyecto incluido dentro de la línea estratégica L5 “Ciberseguridad”.

Los fondos europeos que sustentarán parte de este contrato estarán asociados a la palanca IV “Una administración para el siglo XXI” y en concreto al componente 11 “Modernización de las Administraciones Públicas”, inversión 3 “Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas y las Entidades Locales” del Plan de Recuperación, Transformación y Resiliencia dentro del marco del Mecanismo de Recuperación y Resiliencia del Ministerio de Hacienda y Función Pública para la transformación digital y modernización de las comunidades autónomas.

Este proyecto tiene como principal actividad la implantación de un segundo nivel de firewall en la seguridad perimetral de los CPDs corporativos. Este contrato permite implementar un segundo nivel de firewall que incrementará significativamente las garantías de protección de los sistemas de información e infraestructuras tecnológicas ante amenazas externas.

El indicador de este contrato asociado al proyecto es “Actividad 1-I1 Implantación segundo nivel firewall” siendo su descripción la definida a continuación: El segundo nivel de firewall se ha implementado y presta servicio adecuadamente, filtrando todo el tráfico de la red y contribuyendo adecuadamente a garantizar la seguridad de la información y los servicios.

Objetivos del proyecto:

El colectivo objetivo de este proyecto es la Administración de la Comunidad Autónoma de Cantabria, incluyendo los sistemas de información e infraestructuras tecnológicas en los que se sustentan los procesos internos, así como la prestación del conjunto de servicios que se ofrecen a la ciudadanía, presencialmente o vinculados a la “e-Administración”.

Los principales objetivos específicos de este proyecto son los siguientes:

- Apoyo a la transición Digital (Objetivo 4 del Plan de Recuperación, Transformación y Resiliencia)
- Mejora de la accesibilidad de los servicios (Objetivo 1 del componente 11)
- Mejora la eficiencia y eficacia de los empleados púbicos (Objetivo 3 del componente 11).
- Incrementar el número de procedimientos digitales (Objetivo 1 del Plan Digital de Administraciones Públicas)
- Ciberseguridad (Objetivo L5 de la línea estratégica)

Objetivos CID:

En cuanto a los objetivos determinados en la Decisión de Ejecución del Consejo (Objetivos CID) este proyecto se enmarca dentro del objetivo 168 “Adjudicación de proyectos de apoyo a la transformación digital del Ministerio de Política Territorial y Función Pública y de las Administraciones de las Comunidades Autónomas” que tiene asociada una fecha fin de cumplimiento el T2 de 2025.

Plan antifraude:

El enlace para consultar el plan antifraude del órgano de contratación: https://www.cantabria.es/web/consejeria-de-presidencia-y-justicia/antifraude-fondos-europeos

Contribución climática y digital:

Con respecto a la contribución a la transición climática, cabe indicar que el proyecto asociado a este contrato, asociado a la inversión 3 del componente 11, no contribuye a la transición climática, participando únicamente en la transición digital, considerándose un campo de contribución digital del 100%. A este respecto se adjunta al presente contrato el test de autoevaluación asociado al principio DNSH (Do Not Significant Harm) Autoevaluacion DNSH doble barrera FW.report.pdf

Cumplimiento Orden HFP/1030/2021, de 29 de septiembre.

Con respecto a los test referenciados en la citada orden y teniendo en cuenta la respuesta dada por la Secretaría General de Presidencia, Justicia, Seguridad y Simplificación Administrativa, desde esta Dirección General se asumen como válidas todas las respuestas indicadas, y recogidas en los anexos adjuntos a la presente memoria (ANEXO II.B.1 Test aspectos esenciales, ANEXO III A.- Test conflicto de interés, prevención del fraude y la corrupción y Anexos de Gestión de Hitos y Objetivos Definición de Proyectos y Subproyectos). A este respecto se adjunta al presente contrato el análisis de riesgos de contratación asociado a este contrato Analisis Riesgos contratación doble barrera FW.report.pdf

DACI

Se adjuntan a este expediente el DACI firmado todos los participantes de la DGI en el proyecto DACI DGI.report.pdf.

6. RESPONSABLE DEL CONTRATO

El Coordinador TIC responsable del Área de Comunicaciones del Centro de Proceso de Datos o aquella persona designada por el órgano de contratación a propuesta de la Dirección General de Informática, de la Consejería de Presidencia, Justicia, Seguridad y Simplificación Administrativa.

Sin perjuicio de las facultades y atribuciones que corresponden a otros órganos, y particularmente a la unidad administrativa encargada del seguimiento y de la ejecución del contrato, corresponde al responsable del contrato, entre otras, realizar las funciones siguientes:

- Dictar instrucciones para la correcta realización de la prestación.
- Supervisar las obligaciones asumidas por el contratista.
- Comunicar al órgano de contratación, y al Departamento competente, cualquier cuestión relevante en relación a incidencias o incumplimientos de las cláusulas sociales incorporadas en el contrato, así como las funciones previstas en el artículo 22 del Decreto 75/2019, de 23 de mayo.
- Proponer la suspensión y resolución del contrato o adopción de otras medidas para garantizar su cumplimiento.
- Proponer modificaciones.
- Requerir al contratista datos relativos a las condiciones laborales de los trabajadores, en su caso.
- Comprobar la obligación de pago a subcontratistas, en su caso.
- Controlar la correcta ejecución del contrato.
- Supervisar que los suministros no son defectuosos.
- Proponer la aplicación de penalidades por incumplimiento parcial, cumplimiento defectuoso y demora en la ejecución del contrato.
- Controlar el cumplimiento de las condiciones especiales de ejecución establecidas en este pliego.
- Informar al órgano de contratación sobre cualquier otra anomalía que observe en el contrato durante la ejecución.

7. CLASIFICACIÓN

Se identifica el objeto del contrato con la siguiente codificación según el vocabulario común de contratos públicos (CPV):

- 32500000-8: Equipo y material para telecomunicaciones
- 48781000-6: Paquetes de software de gestión de sistemas

8. JUSTIFICACIÓN DE INSUFICIENCIA DE MEDIOS

La D.G. de Informática no puede asumir con medios propios este contrato, debido a que se trata de un suministro de material específico.

9. PRESUPUESTO BASE DE LICITACIÓN

El presupuesto base de licitación de este contrato es de **800.000 € (IVA incluido)**.

Se entenderá, a todos los efectos, que el importe del contrato incluye todos los gastos directos e indirectos que el contratista deba realizar para la normal ejecución del contrato y cualquier otros que resulten de aplicación según las disposiciones vigentes, así como toda clase de impuestos y licencias.

De acuerdo con lo establecido en el artículo 100.2 de la "Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público", el presupuesto base se desglosa en:

- Costes directos: 85%
  - Equipamiento: 80%
  - Suministro e instalación: 5%

- Costes indirectos: 15%
  - Personal: 1,4% *
  - Gastos generales y beneficio industrial: 8,6 % **
  - Gastos de la red de alianzas comerciales: 5% ***

* Costes de personal "tipo" en una empresa tecnológica. No se incluyen al departamento de investigación, desarrollo e innovación.

** Beneficio medio (en %) de una empresa "tipo" fabricante de elementos tecnológicos de la misma categoría que los del objeto del contrato.

*** Gastos asociados a la red de entidades empresariales o comerciales con los que se mantienen acuerdos que posibilitan el acceso a determinados servicios o productos.

10. VALOR ESTIMADO

El valor estimado del contrato es **661.157,03 € (IVA no incluido)**.

Importe calculado conforme determina el artículo 101.7 y 101.10 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, teniendo en cuenta los precios habituales en el mercado en el momento de inicio del procedimiento de adjudicación del contrato y los suministros previos que se han realizado a esta Consejería para este tipo de elementos.

11. FINANCIACIÓN, APLICACIÓN PRESUPUESTARIA Y ANUALIDADES

Este contrato se cofinanciará con cargo a las siguientes partidas presupuestarias:

Aplicación presupuestaria	Anualidad	Importe
02.11.491M.626	2025	138.842,97 €
02.11.140A.626	2025	661.157,03 €

El programa 491M está asociado al gasto operativo de la DG de Informática.

El programa 140A está asociado al Mecanismo de Recuperación y Resiliencia.

Este proyecto se cofinanciará con FONDOS EUROPEOS DEL MECANISMO DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA. El contrato se financia en su totalidad (con la excepción del IVA) mediante los recursos financieros derivados del Instrumento Europeo de Recuperación (Next Generation EU), a través del Mecanismo de Recuperación y Resiliencia establecido por el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, no pudiendo ser financiadas las mismas actuaciones por otros instrumentos y fondos de la Unión Europea.

Aportación de la Comunidad Autónoma de Cantabria:

- El IVA del contrato se financiará mediante financiación propia de la DG de Informática, a través de su presupuesto ordinario.

Desglose:

- Importe total de licitación: 800.000 € (100 %)
  - Importe cofinanciado con fondos europeos: 661.157,03 € (82,64 %)
  - Importe cofinanciado con fondos propios de la CCAA: 138.842,97 € (17,36%)
- IVA total del proyecto: 138.842,97 € (17,36 %)

12. DURACIÓN

El plazo máximo de ejecución del suministro será de 20 semanas. Este plazo comenzará al día siguiente de la formalización del contrato.

13. LUGAR Y PLAZO DE ENTREGA DEL SUMINISTRO

- Lugar y forma de entrega: en las diferentes instalaciones del Centro de Proceso de Datos del Gobierno de Cantabria (Santander) que se indiquen al adjudicatario
- Plazo de entrega: el suministro deberá estar ejecutado a las 20 semanas de la formalización del contrato.

14. ELECCIÓN DEL PROCEDIMIENTO DE ADJUDICACIÓN

Procedimiento abierto.

15. SOLVENCIA ECONÓMICA Y FINANCIERA

Solvencia económica y financiera

La solvencia económica y financiera se acreditará según lo previsto en el artículo 87.1.a) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por considerarse lo más adecuado para la naturaleza del contrato.

El criterio para la acreditación de la solvencia económica y financiera será el volumen anual de negocios referido al mejor ejercicio dentro de los tres últimos disponibles en función de las fechas de constitución o de inicio de actividades del empresario y de presentación de las ofertas por importe igual o superior al exigido en el anuncio de licitación y en los pliegos del contrato.

La solvencia económica quedará acreditada mediante certificación o nota informativa de las cuentas anuales expedida por el registrador mercantil y documentación similar que acredite el depósito en el registro oficial. Los empresarios individuales no inscritos en el Registro Mercantil acreditarán su volumen anual de negocios mediante sus libros de inventarios y cuentas anuales legalizados por el Registro Mercantil.

El requisito mínimo será el volumen anual de negocios, referido al año de mayor volumen de negocios de los tres últimos años concluidos, que deberá ser al menos 1,5 veces el valor estimado del contrato (**991.735,55 €**).

Solvencia técnica o profesional

La solvencia técnica o profesional se acreditará según lo previsto en el artículo 89.1.a) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por considerarse lo más adecuado para la naturaleza del contrato.

Se deberá aportar una relación de los principales suministros realizados de igual o similar naturaleza que los que constituyen el objeto del contrato en el curso de como máximo, los tres últimos años, en la que se indique el importe, la fecha y el destinatario, público o privado de los mismos; cuando sea necesario para garantizar un nivel adecuado de competencia, los poderes adjudicadores podrán indicar que se tendrán en cuenta las pruebas de los suministros pertinentes efectuados más de tres años antes. Cuando le sea requerido por los servicios dependientes del órgano de contratación, los suministros efectuados se acreditarán mediante

certificados expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público; cuando el destinatario sea un sujeto privado, mediante un certificado expedido por este o, a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación; en su caso estos certificados serán comunicados directamente al órgano de contratación por la autoridad competente.

Se tomará como criterio de correspondencia entre los suministros efectuados por el empresario y los que constituyen el objeto del contrato los tres primeros dígitos de los códigos CPV de este contrato: 32500000-8 Equipo y material para telecomunicaciones y 48781000-6: Paquetes de software de gestión de sistemas

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 (**462.809,92 €**).

16. CRITERIOS DE ADJUDICACIÓN

De acuerdo con lo establecido en el artículo 145 de la LCSP, los criterios de adjudicación en base a la mejor relación calidad-precio, se regularán por lo indicado a continuación. Todos los criterios elegidos hacen referencia a características del objeto del contrato y son criterios evaluables de forma automática por aplicación de fórmulas. Se incluirá en un mismo sobre la oferta que incluirá el precio y la respuesta al resto de criterios dependientes de valoración objetiva:

1. PRECIO

Se valorará con un máximo de 90 puntos la oferta más económica. Las demás ofertas se valorarán de acuerdo a la siguiente fórmula:

$$P = Pm \times \frac{90}{Po}$$

P: Puntuación oferta a valorar

Po: Precio oferta a valorar

Pm: Precio oferta más baja

2. AMPLIACIÓN PERIODO DE GARANTÍA

Se valorará con 10 puntos la extensión por 1 año del periodo de garantía mínima exigido en el Pliego de Prescripciones Técnicas en el apartado 2.5 “Garantía de la solución completa” (3 años).

17. FORMA DE PAGO

El pago se realizará una vez realizado el correspondiente suministro, efectivamente entregado y formalmente recibido por parte de la Administración mediante acta de recepción del responsable del contrato, tras la presentación de factura correspondiente, que deberá ser conformada previamente por el responsable del contrato con el Vº. Bº del Director General de Informática.

En todo caso, en materia de recepción, se atenderá a lo dispuesto en las leyes de Presupuestos Generales de la Comunidad Autónoma de Cantabria.

18. SUBCONTRATACIÓN

Se permite la subcontratación del transporte e instalación del hardware asociado al contrato en las dependencias del Centro de Proceso de Datos del Gobierno de Cantabria.

El resto de elementos se consideran la parte esencial del contrato, que es el suministro de unos elementos determinados que deberán ser ofrecidos por el adjudicatario y que constituyen una unidad funcional única, crítica en su conjunto, constituyendo su suministro una tarea crítica que debe ser ejecutada directamente por el adjudicatario, no incluyendo ningún tipo de prestación adicional que pudiera ser susceptible de prestarse por un tercero.

19. PLAZO DE GARANTÍA

3 años a partir de la recepción del contrato.

20. CESIÓN

Este contrato no es susceptible de cesión conforme al artículo 214 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por las características del objeto de este suministro (Suministro de elementos para solución de firewall en Centro Proceso de Datos secundario).

21. CONDICIONES ESPECIALES DE EJECUCIÓN

Se establecen las siguientes consideraciones de tipo social y medioambiental como condiciones especiales de ejecución del contrato:

- La empresa adjudicataria está obligada a favorecer la estabilidad en el empleo, asegurar la igualdad de oportunidades entre hombres y mujeres, contribuir a la integración laboral de los colectivos más desfavorecidos, de manera acorde con la legislación vigente en materia laboral y en cumplimiento de las cláusulas específicas de este contrato.

- La empresa contratista, en el caso de que no esté legalmente obligada a la elaboración del plan de igualdad entre hombres y mujeres, tendrá que presentar, en el plazo máximo de diez días posteriores a la fecha de formalización del contrato, una declaración responsable sobre las medidas aplicables en relación con las personas trabajadoras que participarán en la ejecución del contrato, para alcanzar la igualdad de trato y de oportunidades entre mujeres y hombres en el ámbito laboral, eliminar estereotipos y fomentar una igualdad efectiva y real entre mujeres y hombres.

- La empresa adjudicataria aportará en el plazo máximo de diez días posteriores a la fecha de formalización del contrato, una declaración responsable sobre las medidas aplicables en la ejecución del contrato para garantizar la igualdad de oportunidades y no discriminación de las personas LGTBI, tanto si es el caso entre el personal que ejecuta el contrato como entre las personas destinatarias de la prestación. Las medidas, acordes con el objeto del contrato y la legislación vigente en esta materia, podrán consistir en formación en contenidos relacionados con las discriminaciones que pueden sufrir las personas LGTBI y en el conocimiento de la diversidad con respecto a la orientación sexual, la identidad de género y la expresión de género.

- La totalidad de los embalajes serán reciclables o reutilizables, con la finalidad de promocionar el reciclado de productos y el uso de envases reutilizables.

- Adicionalmente, cabe indicar que el proyecto asociado a este contrato, asociado a la inversión 3 del componente 11, no contribuye a la transición climática, participando únicamente en la transición digital, considerándose un campo de contribución digital del 100%. A este respecto se adjunta al presente contrato el test de autoevaluación asociado al principio DNSH (Do Not Significant Harm): *Autoevaluacion_DNSH_doble_barrera_FW.report*

22. RÉGIMEN DE PENALIDADES DISTINTAS AL ESTABLECIDO CON CARÁCTER GENERAL

Serán de aplicación las especificadas en los artículos 192 a 194, 202 y 217 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y, de forma específica, las siguientes:

a) Incumplimiento de las condiciones especiales de ejecución: Se establece como penalidad la cuantía correspondiente al 0,5% del precio del contrato (IVA excluido) por cada día de incumplimiento.

b) Incumplimiento parcial y defectuoso: Se establece como penalidad la cuantía correspondiente al 2% del precio del contrato (IVA excluido) por incumplimiento parcial de las obligaciones y de las condiciones del suministro previstas en el presente Pliego y en el Pliego de Prescripciones Técnicas.

c) Además, de acuerdo a lo dispuesto en los artículos 193 y 194 de la LCSP, cuando el contratista por causas imputables al mismo incurra en demora respecto al cumplimiento de los plazos de entrega del contrato, podrá ser objeto de la imposición de una penalidad diaria en la proporción de 0,60 euros por cada 1.000 euros del precio del contrato, IVA excluido.

d) Cada vez que las penalidades por demora en la entrega de los suministros objeto del presente contrato alcancen un múltiplo del 5% del precio del contrato, el órgano de contratación estará facultado para proceder a la resolución del mismo o acordar la continuidad de su ejecución con imposición de nuevas penalidades.

e) Por incumplimiento del principio de no causar daño significativo al medio ambiente (principio DNSH) y su normativa de aplicación: se impondrá una penalidad del 5% del precio del contrato, IVA excluido, por cada incumplimiento.

f) Por no suministrar la información a la que se refiere el artículo 22 del 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: se impondrá una penalidad del 5% del precio del contrato, IVA excluido, por cada incumplimiento.

g) En lo relativo a la seguridad de la información, se establece lo dispuesto en el anexo I del presente documento.

La aplicación y pago de estas penalidades no excluye la indemnización a que el órgano de contratación pueda tener derecho por daños y perjuicios ocasionados por incumplimiento imputable al contratista.

23. CAUSAS ESPECIALES DE RESOLUCIÓN, EN SU CASO, CONFORME A LOS ARTÍCULOS 193 Y 195 DE LA LCSP

La acumulación de penalidades, cuando el conjunto de las mismas supere el 50 por ciento del precio del contrato, será causa de resolución del contrato.

En el caso de haberse impuesto dos penalidades por alguna de las causas señaladas en las letras e) y f) del apartado anterior, un nuevo incumplimiento de la misma naturaleza será causa de resolución contractual.

Además, en aplicación del artículo 18 del Decreto 75/2019 de 23 de mayo, por el que se establecen las directrices de política general sobre la incorporación de criterios y cláusulas sociales en la contratación del sector público de la Comunidad Autónoma de Cantabria, serán causas de resolución del contrato:

1. El incumplimiento de las obligaciones previstas en relación a la prevención de riesgos laborales del personal adscrito a la ejecución del contrato y a la subcontratación.
2. El incumplimiento de las condiciones especiales de ejecución previstas en la documentación contractual.
3. El incumplimiento de las condiciones especiales de ejecución previstas en los pliegos
4. El incumplimiento del deber de afiliación y alta en la Seguridad Social del personal que ocupe en la ejecución del contrato.
5. La infracción de las condiciones establecidas para proceder a la subcontratación, así como la falta de acreditación de la aptitud del subcontratista.
6. La falta de veracidad en la información entregada por el órgano de contratación relativa a los datos sobre la subrogación de personal.

7. MODIFICACIONES

No se admiten.

8. SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

En este punto se da cumplimiento al examen de las medidas y requisitos técnicos de ciberseguridad que se exigen al producto objeto de la licitación.

En cuanto al examen del objeto del contrato con respecto al cumplimiento del "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad", del "Decreto 79/2021, de 30 de septiembre por el que se regula la Política Integral de Seguridad de la Información y la Organización competencial para la Protección de Datos Personales de la Administración de la Comunidad Autónoma de Cantabria" y el resto de normativa de aplicación en esta materia, se detallan en la tabla siguiente las características clave del objeto del contrato siguiendo las tablas resumen del anexo IV Orden PRE/59/2018, de 2 de noviembre:

Arts.	FACTOR CLAVE PCAP	VALOR	OBSERVACIONES
4/11	¿El objeto del contrato implica el acceso a información de la ACAC?	No	
5/12	¿El objeto del contrato incluye el tratamiento de información de la ACAC?	No	
	¿Incluye el tratamiento de datos personales?	No	
6/13	¿El objeto del contrato implica el acceso a sistemas de información de la ACAC por parte de personal del adjudicatario?	No	
	¿El acceso a los sistemas implica que el personal del adjudicatario accede a información de la ACAC?	No	
7/14	¿El objeto del contrato corresponde a un suministro de aplicaciones realizada a medida y su período de mantenimiento correspondiente?	No	
	¿El suministro implica que el personal del adjudicatario accede a información de la ACAC?	**Sí**	
	¿El suministro implica que el personal del adjudicatario acceda a sistemas de información de la ACAC?	No	
8/15	¿El objeto del contrato corresponde a la prestación de un soporte tecnológico avanzado?	No	
9/16	**¿El objeto del contrato implica el suministro de aplicaciones comerciales o de elementos hardware?**	**Sí**	
	¿El objeto del contrato implica la subscripción a servicios tecnológicos?	No	
10/17	¿Es un contrato integral de soporte tecnológico u otro tipo de contrato relacionado con la tecnología?	No	
Arts.	**FACTOR CLAVE PPT**	**VALOR**	**OBSERVACIONES**

11	¿Es un contrato de prestación de servicios cuyo objeto no implique el acceso a información ni a sistemas de información de la Administración de la Comunidad Autónoma de Cantabria.?	No	
12	¿Es un contrato cuyo objeto incluye el tratamiento de información?	No	
13	¿Es un contrato cuyo objeto implique el acceso a sistemas de información de la Administración de la Comunidad Autónoma de Cantabria por parte del personal del adjudicatario?	No	
14	¿Es un contrato cuyo objeto implique suministro de aplicaciones software realizadas a medida?	No	
15	¿Es un contrato cuyo objeto incluya la prestación de un soporte tecnológico avanzado?	No	
16	**¿Es un contrato cuyo objeto implique el suministro de aplicaciones comerciales o de elementos hardware, así como suscripción de servicios tecnológicos?**	**Sí**	
17	¿Es un contrato integral de soporte o un contrato de otro objeto relacionado con la tecnología?	No	

*Nota: ACAC significa "Administración de la Comunidad Autónoma de Cantabria".

De este examen del objeto del contrato se establecen diferentes medidas y requisitos técnicos de ciberseguridad que se exigen para los productos objeto de la licitación. Estas medidas y requisitos se encuentran en:

- Pliego de Prescripciones Técnicas:
    - Apartado 3, Cláusulas sobre seguridad de la información y protección de datos personales.
- ANEXO I de esta memoria:
    - Cláusulas a incluir en el PCAP.

Finalmente, cabe indicar que el objeto del contrato es el suministro de elementos de una solución de firewall, por lo tanto, deberán estar certificados como “Categoría Alta” del Esquema Nacional de Seguridad.

9. PROPUESTA DE AUTORIZACIÓN DEL GASTO

Se propone autorizar un gasto por el importe de licitación de este contrato de **800.000 € (IVA incluido)**. Este contrato se financiará con cargo a las partidas presupuestarias y en las anualidades previstas en esta memoria.

10. PROPUESTA DE CONTRATACIÓN

Por todo lo cual, esta Dirección General de Informática PROPONE el inicio de un expediente de contratación de suministro para cubrir las necesidades indicadas. Dadas las condiciones específicas del contrato reflejadas en el pliego de prescripciones técnicas, se proponen únicamente criterios evaluables de forma automática por aplicación de fórmulas.

Santander, a fecha de la firma electrónica

LA COORDINADORA DE ÁREA TIC	EL JEFE DE SERVICIO DEL CENTRO DE PROCESO DE DATOS	CONFORME EL DIRECTOR GENERAL DE INFORMÁTICA
Fdo.: Olga Esteras Hernández	Fdo.: Alfredo Jaime Fernandez	Fdo.: Pablo Izu Morales

SECRETARIA GENERAL DE PRESIDENCIA, JUSTICIA, SEGURIDAD Y SIMPLIFICACIÓN ADMINISTRATIVA

ANEXO I – Cláusulas orden PRE/59/2018, de 2 de noviembre, para el PCAP

Cláusulas de la orden PRE/59/2018, de 2 de noviembre, por la que se regulan las condiciones sobre seguridad de la información y protección de datos personales a incorporar en los Pliegos de Cláusulas Administrativas Particulares y de Prescripciones Técnicas en la contratación pública de la Administración de la Comunidad Autónoma de Cantabria.

- Protección de datos de carácter personal relativos a la gestión del contrato:

Ambas partes quedan informadas que los datos de representantes o personas de contacto de las mismas, incluidos en el presente contrato o facilitados entre ellas con motivo de su ejecución, serán objeto de tratamiento de datos personales por cada una de ellas, con la finalidad de realizar la gestión de la relación contractual.

Cada parte dará la información oportuna sobre el tratamiento a los titulares de tales datos y les reconoce la posibilidad de ejercitar gratuitamente los derechos que la legislación vigente en materia de protección de datos personales otorga a los interesados.

- Deber de confidencialidad en el acceso fortuito a información:

- Si el adjudicatario accediera fortuitamente a información de la Administración de la Comunidad Autónoma de Cantabria que no esté relacionada con el objeto del contrato tiene obligación de guardar estricta confidencialidad sobre la misma e informar al órgano de contratación sobre el hecho acontecido.

- El adjudicatario deberá informar fehacientemente a su personal sobre esta obligación.

- Régimen de penalidades complementario al establecido con carácter general para el presente contrato: porcentajes a aplicar.

1. El órgano de contratación estará facultado para la imposición de las siguientes penalidades asociadas al incumplimiento de obligaciones relativas a seguridad de la información contenida en este Pliego de Cláusulas Administrativas Particulares y/o en el Pliego de Prescripciones Técnicas.
2. Cuando el incumplimiento por parte del adjudicatario pudiera dar origen a un incidente correspondiente a la siguiente escala de niveles:
    a) Alto, la penalidad será del 10%
    b) Medio, la penalidad será del 5%
    c) Básico, la penalidad será del 2.5%

    Este porcentaje se aplicará sobre el importe de la factura correspondiente al período en el que tiene lugar el incumplimiento.

3. Si, una vez impuestas 3 penalidades de nivel bajo, 2 de nivel media o 1 de nivel alto, se produjera un nuevo incumplimiento del mismo nivel, se impondrá una nueva penalidad por reiteración, que será del 15% sobre el importe de la factura correspondiente al período en el que tiene lugar el incumplimiento.

   Si, una vez impuesta la penalidad por reiteración, se produjera otro nuevo incumplimiento de cualquier nivel, el órgano de contratación estará facultado para proceder a la resolución del contrato.

   Los incidentes de seguridad y las penalidades a aplicar seguirán los mismos criterios tanto si están relacionados con tratamientos automatizados, con tratamientos no automatizados o tratamientos mixtos.

   En aquellos incidentes de seguridad en los que concurran varias circunstancias que permitirían determinar diferentes niveles según el criterio aplicable, se considerará del nivel más alto entre todos los posibles.

<u>- Niveles de los incidentes de seguridad relacionados con tomas de control, alternaciones de la configuración o que afecten a las dimensiones de autenticidad o trazabilidad.</u>

En base a los criterios del Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para la determinación de la categoría de los sistemas de información, y en lo relativo a tomas de control, alteraciones de la configuración, así como alteración de las dimensiones de autenticidad y trazabilidad:

- Se considerarán incidentes de seguridad de nivel ALTO, cuando estén afectados:
  - 1 o más sistemas de información de categoría ALTA.
  - Más de 10 sistemas de información de categoría MEDIA.
  - Más de 50 sistemas de información de categoría BÁSICA.

- Se considerarán incidentes de seguridad de la información de nivel MEDIO, cuando se vean afectados:
  - 1 o más sistemas de información de categoría MEDIA.
  - Más de 20 sistemas de información de categoría BÁSICA.
- Se considerarán incidentes de seguridad de la información de nivel BASICO, cuando se vean afectados:

- 1 o más sistemas de información de categoría BÁSICA.

<u>- Niveles de los incidentes de seguridad que afecten a la dimensión de continuidad.</u>

En base a los criterios del Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para la determinación de la categoría de los sistemas de información, y en lo relativo a la dimensión de continuidad (suspensión del funcionamiento de los sistemas de información o impedimento para acceder a la información que contienen):

- Se considerarán incidentes de seguridad de nivel ALTO, cuando el incidente dure un tiempo superior a 24 horas y estén afectados:
  - 1 o más sistemas de información de categoría ALTA.
  - Más de 10 sistemas de información de categoría MEDIA.
  - Más de 50 sistemas de información de categoría BÁSICA.
- Se considerarán incidentes de seguridad de la información de nivel MEDIO, cuando el incidente dure más de 72 horas y se vean afectados:
  - 1 o más sistemas de información de categoría MEDIA.
  - Más de 20 sistemas de información de categoría BÁSICA.
- Se considerarán incidentes de seguridad de la información de nivel BASICO, cuando el incidente dure más de 96 horas y se vean afectados:
  - 1 o más sistemas de información de categoría BÁSICA.

<u>- Niveles de los incidentes de seguridad que afecten a la reputación de la Administración de la Comunidad Autónoma de Cantabria.</u>

- Los incidentes de seguridad que afecten a la reputación de la Comunidad Autónoma de Cantabria serán considerados:
  - De nivel ALTO cuando se produzcan daños reputacionales de difícil reparación, con una amplia cobertura en los medios de comunicación y/o que afecten a la reputación de terceros.
  - De nivel MEDIO, cuando se produzcan daños reputacionales apreciables, aunque reparables, con una amplia cobertura en los medios de comunicación y que no afecten a la reputación de terceros.

- De nivel BÁSICO, cuando se produzcan daños reputacionales puntuales, sin una amplia cobertura en los medios de comunicación y que no afecten a la reputación de terceros.

<u>-Seguridad en el acceso a los sistemas de información de la Administración de la Comunidad Autónoma de Cantabria.</u>

El adjudicatario deberá informar de forma fehaciente al personal adscrito a la ejecución del contrato, que vaya a acceder a los sistemas de información de la Administración de la Comunidad Autónoma de Cantabria, sobre las cláusulas de confidencialidad y seguridad del presente pliego, sobre la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria, así como de las normas de seguridad de la información o procedimientos de seguridad de la información que les afecten.

- El adjudicatario, en lo relativo al contenido y alcance del presente contrato, deberá aceptar la realización de auditorías sobre seguridad de la información por parte de la Administración de la Comunidad Autónoma de Cantabria.
- El adjudicatario y el personal adscrito a la ejecución del contrato deberán informar a la Administración de la Comunidad Autónoma de Cantabria de aquellos incidentes de seguridad o debilidades potenciales, que detecten durante la prestación del mismo.
- Por norma general, la asignación de credenciales será individualizada, con un uso estrictamente personal e intransferible. De forma excepcional, en aquellos casos en que no pueda realizarse una asignación individualizada de credenciales, debido a las características del servicio, debe quedar identificada singularmente cada persona que haga uso de las credenciales de acceso al sistema. Para ello el adjudicatario deberá:
  - Establecer los mecanismos internos que sean oportunos para contar con un listado permanentemente actualizado de las personas que utilicen cada credencial de acceso no individualizada en cada momento, para que la trazabilidad quede garantizada.
  - Proporcionar a la Administración de la Comunidad Autónoma de Cantabria, siempre que lo solicite, información precisa de las personas que han utilizado cada credencial de acceso no individualizada en un momento dado o a lo largo de cierto periodo.

- Velar por que cada credencial no individualizada exclusivamente sea accesible o conocida por el personal que va a prestar el servicio, el cual deberá estar informado sobre la obligación de no entregar o revelar la credencial a ninguna otra persona.

-Requisitos de seguridad de la información y de los sistemas de información

El suministro debe ser compatible con los requisitos de seguridad de la información y de los sistemas de información que estén incluidos en el Pliego de Prescripciones Técnicas.