Pliego de Prescripciones Técnicas Particulares para la elaboración de un "Libro Blanco y Observatorio Sectorial de la Ciberseguridad en Navarra"

Dirección de Tecnologías de la Información y Digitalización

nasertic

Navarra de Servicios y Tecnologías, S.A.

| C/ Orcoyen, s/n. 31011 Pamplona – Navarra
| info@nasertic.es | www.nasertic.es
| Tel: 848 420 500 | Fax: 848 426 751

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

Índice

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

1 CONTEXTO

1.1 Introducción

Las amenazas a la seguridad de la información han existido siempre, pero ha sido en los últimos años cuando los riesgos asociados a las mismas han sufrido un crecimiento exponencial. La adopción de tecnologías como elementos fundamentales en los procesos de negocio influye de forma relevante en el impacto de los ciberataques. Igualmente, junto con el desarrollo de las nuevas tecnologías ha aumentado la complejidad de los sistemas empleados por los atacantes para poner en jaque la información y ha aumentado la probabilidad de que se produzcan estos ataques. Esto provoca que el riesgo al que se ven expuestas las organizaciones sea especialmente alto, dinámico y difícil de gestionar, tal y como nos demuestra conocer a diario nuevas empresas y entidades que han visto su funcionamiento paralizado por ciberataques.

Es necesario tanto innovar en ciberseguridad como acercar la ciberseguridad a un ámbito cada vez más sensible y expuesto: el tejido empresarial. Por un lado, por la rápida evolución de las tecnologías y la necesidad por parte de las organizaciones de adoptarlas para ser cada vez más competitivas y eficientes. Además, es imprescindible mantener el ritmo de innovación en ciberseguridad para poder adoptar nuevas tecnologías sin superar un nivel de riesgo aceptable. Para ello, se deben generar espacios de colaboración regional público-privada, involucrando administración, empresas y academia, para impulsar la innovación, la adopción de soluciones de ciberseguridad y la generación de talento.

1.2 Iniciativas en el ámbito de la ciberseguridad en Navarra

El Gobierno de Navarra no ha sido ajeno a esta realidad, apostando en este ámbito por dos iniciativas de referencia en Navarra:

- **Polo de Innovación Digital de Navarra (Polo IRIS)**: nace con la misión de '*contribuir a la aceleración de la transformación digital de innovación en Navarra, actuando como catalizador y ventanilla única de la digitalización de la región a través de la prestación eficiente de servicios, la gestión eficaz de sus recursos y la generación de espacios de colaboración con los agentes clave público-privados'*. La visión del Polo es la de '*constituirse como el espacio de referencia en materia de digitalización e innovación de Navarra, favoreciendo la colaboración y generación de alianzas entre todos los agentes económicos y sociales de la región e impulsando su transformación a través de servicios avanzados'*. Se puede caracterizar a través de los siguientes pilares fundamentales:
    1. Como respuesta a los retos de transformación digital de la región.
    2. Como ventanilla única de transformación digital e innovación en Navarra.
    3. Como impulsor de la especialización tecnológica en Navarra.
    4. Como catalizador de servicios digitales al tejido empresarial navarro.
    5. Como promotor de una sociedad digital en Navarra.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

Es en el punto tercero, donde el Polo focaliza esfuerzos en el **impulso de áreas de especialización tecnológica** que permitan impulsar la competitividad global de la Comunidad Foral de navarra y que, de forma específica, contribuyan al desarrollo de los sectores estratégicos fijados en la Estrategia de Especialización Inteligente de Navarra S4.

Una de estas áreas de especialización es la **Ciberseguridad**. Abarca todas aquellas actividades o procesos mediante los que los sistemas de información y comunicación y el contenido de los mismos son protegidos de o defendidos contra daños y contra su uso, modificación o explotación no autorizados.

- **Navarra Cybersecurity Center (NavCC)**: Su principal objetivo es el **impulso al desarrollo de iniciativas en torno a la ciberseguridad** que deriven en un aumento de la ciber resiliencia en todos los ámbitos de la Comunidad Foral de Navarra, incluyendo el tejido empresarial y con especial foco en pymes y autónomos y establecerse como ventanilla única en materia de seguridad digital.

  Las iniciativas se dirigen a la dinamización del sector de la ciberseguridad tanto desde el punto de la oferta de los servicios ofrecidos en la Comunidad Foral, como desde el punto de vista de la demanda y utilización de dichos servicios. Por tanto, tiene como objetivo estratégico contribuir a la transformación socioeconómica sostenible de Navarra en un entorno digital e hiperconectado, seguro y ciberresiliente.

Ambas iniciativas están íntimamente relacionadas, siendo el NavCC el principal instrumento para el desarrollo del área de especialización de ciberseguridad del Polo de Innovación Digital de Navarra IRIS.

1.3 Objetivos estratégicos en Ciberseguridad para el tejido empresarial navarro

En este apartado se definen las bases estratégicas del área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra para potenciar este ámbito.

La transversalidad y globalidad del ciberespacio supone que la ciberseguridad sea un tema clave en todos los sectores de actividad. Precisamente por ello la cooperación y compartición de avances y conocimiento permiten mayores logros en la protección frente a las ciber amenazas. La ciberseguridad tiene un carácter transversal que afecta a todo el tejido empresarial, pero también a Administraciones Públicas y a la sociedad en su conjunto. Por tanto, el área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra, entendiendo la ciberseguridad como una oportunidad económica, profesional y empresarial, se centra en potenciar iniciativas tractoras con potencial para escalado en distintos sectores industriales y productivos, incluyendo también acciones relacionadas con la sensibilización respecto a los riesgos inherentes al mundo conectado.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

Con todo lo anterior, podemos definir los siguientes **objetivos estratégicos en materia de ciberseguridad, canalizados a través del Navarra Cybewrsecurity Center (área de especialización del Polo IRIS)**:

1. Contribuir, desde el impulso público, a que el proceso de digitalización y la hiperconectividad en un entorno ciberseguro produzcan una transformación socioeconómica sostenible en términos de **productividad y empleo**.

2. Impulsar proyectos regionales de ciberseguridad, asegurando su eficiencia y maximizando su impacto a través de la **coordinación, la colaboración y la complementariedad** de la colaboración público-privada.

3. Impulsar el **equilibrio territorial** en materia de ciberseguridad, de modo que ningún ámbito se quede rezagado en un objetivo global como el impulso a la cultura de la ciberseguridad para empresas y ciudadanía.

4. Fomentar el crecimiento estratégico de un **sector clave como el TIC**, pero también otros **sectores económicos estratégicos** en las economías regionales a través de la transformación y especialización digital.

5. Establecer las bases para un **entorno de colaboración estable y sostenible** a medio y largo plazo que velen por el avance coordinado en aspectos de ciberseguridad.

Para el desarrollo de los objetivos estratégicos anteriores, se han definido las siguientes **líneas de actuación**:

1. Creación de un centro de ciberseguridad regional.
2. Fomento del ecosistema empresarial en el sector de la ciberseguridad.
3. Creación de centros demostradores.
4. Gestión del talento.
5. Acciones de sensibilización.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

2 OBJETO Y OBJETIVOS DE LA CONTRATACIÓN

2.1 Objeto

El objeto del presente pliego es definir las prescripciones técnicas particulares necesarias para la licitación del servicio de elaboración de un "**Libro Blanco y Observatorio Sectorial de la Ciberseguridad en Navarra**", detallando su alcance objetivo, así como los requisitos mínimos y condiciones técnicas generales que deberán considerarse para la prestación del servicio.

El "**Libro Blanco y Observatorio Sectorial de la Ciberseguridad en Navarra**" recogerá un análisis pormenorizado del ecosistema de ciberseguridad en navarra, con un foco especial en la oferta de productos y servicios disponibles en la materia (análisis de la oferta), así como una caracterización del tejido empresarial navarro y sus necesidades en términos de cumplimiento de normativas/regulaciones en el ámbito de la ciberseguridad (análisis de la demanda).

El estudio ofrecerá una perspectiva de ciberseguridad dirigida, no solo a empresas, agencias, instituciones y estudiantes, sino, a todo aquel que busque mantenerse informado sobre el estado y las tendencias actuales en esta materia.

2.2 Objetivos

Los objetivos del servicio son los siguientes:

1. **Análisis del ecosistema de ciberseguridad**, con el fin de ofrecer una perspectiva del estado del arte, las tendencias y los agentes clave que conforman el ecosistema de Ciberseguridad en Navarra.

   El estudio incluirá un análisis de **contexto** del sector de la ciberseguridad a nivel global, europeo, estatal y regional en Navarra. Este análisis incluirá aspectos como valor de mercado, inversiones, empleo, tendencias de ciberseguridad y cibercrimen y el entorno regulatorio.

   Se realizará un mapeo exhaustivo de los **agentes** clave que conforman el ecosistema de ciberseguridad navarro: organismos oficiales, asociaciones, empresas, centros tecnológicos y red de educación/formación.

2. **Análisis de la oferta**, realizando un estudio exhaustivo de las empresas que ofrezcan soluciones en materia de ciberseguridad en Navarra, identificando, clasificando y evaluando sus capacidades reales, y generando un "**Catálogo de Productos y Servicios de Ciberseguridad"** que sirva como guía de referencia estructurada, estandarizada y neutral para las empresas navarras que necesiten hacer uso de estas soluciones.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

La clasificación de los productos y servicios se realizará en base a una taxonomía acordada, que será definida de acuerdo a estándares o marcos ampliamente reconocidos a nivel nacional e internacional.

3- **Análisis de la demanda**, a través de la caracterización del ecosistema empresarial navarro junto con el análisis de las regulaciones y estándares de ciberseguridad de aplicabilidad en función de esta clasificación, generando una "**Guía Normativa de Ciberseguridad"** cuyo objetivo es ofrecer una visión de los requisitos normativos a los que se enfrentan las empresas de los sectores estratégicos navarros.

   Se identificarán las tendencias sectoriales en materia de requerimientos de ciberseguridad, así como las regulaciones y estándares de referencia y las medidas técnicas y organizativas que deban adoptar las empresas navarras de acuerdo a su clasificación. Se hará especial foco en las normas europeas: NIS2 y CRA y su impacto en el tejido empresarial navarro.

4- **Cuadro de mando**, diseño, desarrollo y puesta en marcha de un cuadro de mando interactivo integrado en el portal web del NavCC.

   El cuadro de mando recogerá los datos obtenidos en el estudio ("Catálogo de Productos y Servicios" y "Guía Normativa de Ciberseguridad") de forma procesable dinámica y permitirá definir diferentes vistas que sirvan como herramienta visual de acceso público para el ecosistema navarro de ciberseguridad.

El servicio incluirá, además de la elaboración del libro blanco y el cuadro de mando, una fase de mantenimiento y actualización continuada (hasta Junio de 2026), así como el apoyo en las labores de difusión y comunicación.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

3 DESCRIPCIÓN DEL SERVICIO

En este apartado se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por NASERTIC, cubriendo los aspectos de tareas a realizar y resultados esperados.

Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario) pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. El licitador puede ofertar prestaciones superiores a las solicitadas, que se tendrán en cuenta durante la valoración técnica de la oferta.

El adjudicatario deberá aportar y describir en su oferta los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

El adjudicatario se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la prestación del servicio, respecto a toda la información que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

Para la prestación del servicio, NASERTIC propone ejecutar las siguientes actividades:

3.1 FASE I: Análisis del Ecosistema de Ciberseguridad

El objetivo de esta primera fase es obtener un estado del arte del sector, con datos vigentes y verificables que se utilizarán posteriormente durante el proyecto. Se realizará un análisis del mercado de la ciberseguridad mediante una visión global, europea, estatal y específica de la región de Navarra.

Se realizará un análisis inicial del contexto y estado del arte, que incluirá información relacionada con el valor del mercado, las inversiones, profesionales y empleo, iniciativas de emprendimiento, instrumentos de ayuda a empresas, tendencias dentro del sector e impacto del cibercrimen, entorno regulatorio y censo de eventos especializados en ciberseguridad. Deberán incluirse las referencias de los datos incluidos y se organizarán a nivel internacional, estatal y Navarra.

Posteriormente se llevará a cabo un estudio pormenorizado de los diferentes agentes que conforman el ecosistema de ciberseguridad en Navarra. Para ello se analizarán las entidades privadas y públicas especializadas que se dedican a proveer servicios y soluciones en la materia y se clasificarán de acuerdo a categorías predefinidas como pueden ser: administraciones públicas y organismos oficiales, asociaciones empresariales y empresas especializadas, centros tecnológicos, universidades y centros de formación.

El entregable de esta fase del proyecto será una primera versión parcial del libro blanco de la ciberseguridad en Navarra que ofrezca una visión global del estado del arte.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

3.2 FASE II: Catálogo de Productos y Servicios

En esta fase se realizará un estudio exhaustivo de los agentes que ofrezcan soluciones en materia de ciberseguridad en Navarra, identificando, clasificando y evaluando sus capacidades reales, y generando un "**Catálogo de Productos y Servicios de Ciberseguridad"** que sirva como guía de referencia estructurada, estandarizada y neutral para las empresas navarras que necesiten hacer uso de estas soluciones.

El entregable de esta fase del proyecto será la ampliación del libro blanco de la ciberseguridad en Navarra, incluyendo la información de todos los agentes y el "Catálogo de Productos y Servicios". Además, se entregará toda aquella documentación obtenida como consecuencia del análisis, incluyendo fichas debidamente cumplimentadas de cada uno de los agentes catalogados.

Para la elaboración de esta fase del estudio, se propone ejecutar las siguientes actividades:

- **Caracterización de los Agentes**

Se identificarán los agentes con capacidad para ofrecer productos o servicios de ciberseguridad en el territorio navarro, y se definirá un sistema de categorización de los mismos en base a su naturaleza y características. Para esta categorización se evaluarán aspectos que se consideren relevantes, como por ejemplo el tamaño de la empresa y su volumen de facturación en productos y servicios de ciberseguridad, el ámbito de cobertura territorial, los niveles de especialización sectorial o la tipología de clientes a los que se dirigen (autónomo, PYME o gran empresa).

Es labor de la empresa adjudicataria, teniendo en cuenta la sensibilidad y grado de madurez del sector y de las propias empresas, proponer el contenido de cada una de las categorías, el grado de exigencia a considerar para ubicarse en cada una de ellas y diseñar el proceso de recopilación de la información que permita la correcta clasificación de las mismas.

- **Taxonomía de Productos y Servicios**

Se realizará una clasificación de los productos y servicios en base a una taxonomía acordada, que será definida de acuerdo a estándares o marcos ampliamente reconocidos a nivel nacional e internacional. Esta taxonomía permitirá conocer en detalle los servicios y productos que se encuentren actualmente en el mercado de la ciberseguridad, mediante el uso de un lenguaje común que estandarice la oferta, facilitando así su comprensión y la búsqueda de soluciones por parte de las empresas de la demanda.

- **Análisis y validación de los Agentes y sus capacidades**

Se analizará, de forma exhaustiva, las capacidades de los diferentes agentes y su oferta en relación con el marco estandarizado (taxonomía) de productos y servicios de ciberseguridad. La validación de capacidades se llevará a cabo en base al contacto directo

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

(de forma presencial, telemática, telefónica o por e-mail) y análisis de información recopilada, estableciendo diferentes niveles que determinen el grado de certeza o nivel de confianza en lo que se refiere a la información facilitada por cada uno de ellos.

- **Elaboración del "Catálogo de Productos y Servicios"**

Se elaborará el "Catálogo de Productos y Servicios", que se integrará en el Libro Blanco y ofrecerá la información detallada de los agentes, para entender sus capacidades a nivel de productos/servicios.

La información del catálogo estará preparada para su posterior integración en el cuadro de mando que se desarrollará en la FASE IV, y que permitirá realizar búsquedas y agrupaciones de forma sencilla, para facilitar la búsqueda de proveedores por parte de las empresas de la demanda.

Las empresas incluidas en el catálogo estarán autorizadas para usar el sello de "Empresa registrada en el catálogo de ciberseguridad de Navarra".

3.3 FASE III: Guía Normativa de Ciberseguridad

En esta fase se realizará una caracterización del ecosistema empresarial navarro (la demanda) junto con el análisis de las regulaciones y estándares de ciberseguridad de aplicabilidad, generando una "**Guía Normativa de Ciberseguridad"** cuyo objetivo es identificar los requisitos normativos/regulatorios de los principales sectores de Navarra, identificando los aspectos aplicables y cómo estos deben ser abordados, obteniendo una posición diferencial frente a la propia competencia gracias al cumplimiento de los mismos.

El entregable de esta fase del proyecto será la ampliación del libro blanco de la ciberseguridad en Navarra, incluyendo los estudios sectoriales y la "Guía Normativa de Ciberseguridad". Además, se entregará toda aquella documentación obtenida como consecuencia del análisis, incluyendo fichas debidamente cumplimentadas de cada una de las normativas.

Para la elaboración del estudio, se propone ejecutar las siguientes actividades:

- **Caracterización Sectorial**

Se identificarán las tendencias de los principales sectores de Navarra en materia de ciberseguridad, obteniendo una visión de estado del arte sectorial, con datos vigentes y verificables que se utilizarán posteriormente durante el proyecto.

Para ello se definirá un sistema de categorización de las empresas en base a su naturaleza y características, evaluando aspectos que se consideren relevantes, y se aportarán datos del sector, como pueden ser el número de empresas en Navarra, porcentaje del peso de cada actividad, número de empleados, dimensiones de la industria, PIB, exportaciones, etc.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

Es labor de la empresa adjudicataria proponer el alcance de cada una de las categorías y los requisitos a considerar para ubicarse en cada una de ellas.

Se realizará un estudio pormenorizado sobre el estado de la ciberseguridad (situación actual, principales retos, evolución y tendencias) de, al menos, los siguientes sectores estratégicos: automoción, energético, agroalimentario y pymes.

- **Identificación de la regulación y los estándares de referencia**

Se identificará y analizará la regulación y los estándares de referencia en materia de ciberseguridad que puedan ser de aplicación para los diferentes sectores de interés. El estudio permitirá un posterior análisis e identificación de las necesidades que tienen las empresas en el ámbito de la ciberseguridad.

Para realizar este estudio se consultarán diferentes fuentes de información, incluyendo las asociaciones y clústeres sectoriales, se analizarán las regulaciones y estándares identificados (tanto nacionales como internacionales) y se seleccionarán aquellos de aplicabilidad.

Se realizará un estudio más detallado y resumen ejecutivo de las normativas más relevantes, incluyendo, al menos, NIS2, CRA, GDPR, TISAX y UNECE/R155.

El estudio tendrá en cuenta las normativas internacionales y aquellas que afecten a los principales países de exportación.

- **Análisis y asociación de los requisitos de Ciberseguridad**

Tras la identificación de las regulaciones y estándares de referencia, se deberá plantear un análisis de estos para extraer los requisitos de ciberseguridad a cumplir.

Se realizará un estudio de los requisitos y una descripción de los mismos en lenguaje natural y comprensible.

Se realizará una asociación de los requisitos de ciberseguridad con cada una de las categorías/sectores empresariales identificados en el estudio previo.

- **Elaboración de la "Guía Normativa de Ciberseguridad"**

Se elaborará una "Guía Normativa de Ciberseguridad" que permita a cada empresa navarra conocer, de una manera sencilla, los requisitos a los está sujeta en base a su clasificación por categoría/sector y su grado de internacionalización, así como la regulación/normativa que los impone.

La guía se integrará en el Libro Blanco y la información estará preparada para su posterior integración en el cuadro de mando que se desarrollará en la FASE IV, y que permitirá realizar búsquedas y agrupaciones de forma sencilla, para facilitar la búsqueda por parte de las empresas de la demanda.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

3.4 FASE IV: Cuadro de Mando

Esta fase contemplará el diseño y desarrollo de un cuadro de mando interactivo soportado en PowerBI que permita la visualización de los datos resultado del estudio del libro blanco ("Catálogo de Productos y Servicios" y "Guía Normativa de Ciberseguridad"), en la web del Navarra Cybersecurity Center como "Observatorio sectorial de la ciberseguridad en Navarra".

Este sistema permitirá visualizar todos los datos obtenidos en los puntos anteriores, creando vistas, paneles e informes específicos para cada caso. La fácil usabilidad por parte de los usuarios deberá ser un aspecto esencial.

La empresa licitadora hará una propuesta sobre los contenidos de este cuadro de mando que se consideren más adecuados para ser publicados en la web del NavCC, cómo representarlos y la forma de visualizarlos en función de los diferentes públicos objetivos. Habrá que plantear una visión interna de todos los datos y una visión externa para la que habrá una serie de vistas para poder mostrar de forma publica en la web.

El estilo, diseño y contenidos tienen que estar totalmente alineados con el manual de identidad digital del NavCC. Para ello, se deberán entregar previamente bocetos sujetos a validación por el NavCC al igual que un análisis funcional de la operativa. La puesta en producción y carga de contenidos de este cuadro de mando y del observatorio sectorial de la ciberseguridad en Navarra será responsabilidad de la empresa adjudicataria de este contrato.

3.5 FASE V: Mantenimiento y Actualizaciones

El Catálogo de Productos y Servicios, la Guía Normativa y el Cuadro de Mandos se entienden como herramientas vivas y en constante evolución, es por ello que se requiere actualizar de forma constante la información de la que se nutren. Es labor del adjudicatario, a través de un observatorio y seguimiento continuo de los agentes de la oferta y la demanda, la actualización de los datos al menos cada 6 meses, siendo preferible una actualización más frecuente.

Tras la publicación de la primera edición del Libro Blanco, y a través del observatorio y seguimiento continuo, se publicarán dos actualizaciones del mismo (hasta Junio de 2026).

Para la actualización de alguno de los datos podría ser necesario contactar directamente con los agentes del ecosistema.

Durante la fase de mantenimiento, el adjudicatario ofrecerá un soporte y asesoramiento en caso de dudas y consultas, y apoyará así mismo en las labores de comunicación y difusión de los resultados del servicio.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

3.6 Hitos del Proyecto

La propuesta presentada deberá cumplir con los siguientes hitos para la ejecución de las diferentes fases del proyecto:

- FASE I: Análisis del Ecosistema de Ciberseguridad
  Esta fase deberá quedar entregada y aprobada dentro de los 2 meses siguientes a la adjudicación del servicio.

- FASE II: Catálogo de Productos y Servicios
  Esta fase deberá quedar entregada y aprobada dentro de los 5 meses siguientes a la adjudicación del servicio.

- FASE III: Guía Normativa de Ciberseguridad
  Esta fase deberá quedar entregada y aprobada dentro de los 5 meses siguientes a la adjudicación del servicio.

- FASE IV: Cuadro de Mando
  Esta fase deberá quedar entregada y aprobada dentro de los 8 meses siguientes a la adjudicación del servicio.

- FASE V.1: Primera Actualización
  Esta fase deberá quedar entregada y aprobada antes del 31 de Diciembre de 2025.

- FASE V.II: Segunda Actualización
  Esta fase deberá quedar entregada y aprobada antes del 31 de Mayo de 2026.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

4 METODOLOGÍA Y PLAN DE TRABAJO

La empresa licitadora deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, cumpliendo los objetivos y características fijados en el presente pliego (3 DESCRIPCIÓN DEL SERVICIO). En la metodología la empresa licitadora deberá detallar la forma en la que abordará cada una de las fases definidas para el proyecto. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

Para el desarrollo del cuadro de mando, como mínimo la metodología debe detallar las diferentes fases de definición, carga de contenido, pruebas y puesta en producción.

Entendemos que varias de las actividades del contrato se podrían simultanear en el tiempo, dado que son actividades independientes, pero dejamos a criterio del adjudicatario la planificación y organización, siempre y cuando se cumplan los hitos de entrega (3.6 Hitos del Proyecto) en los tiempos especificados.

La empresa licitadora deberá presentar un plan de trabajo que incluya al menos las tareas, hitos y entregables asociados a los trabajos. Dichas propuestas deberán estar basada en su experiencia y se incluirá una descripción que detalle cada tarea definiéndola con un grado de profundidad que permita comprender su alcance.

5 EQUIPO DE TRABAJO

El equipo estará formado por el número de profesionales, perfiles y dedicaciones que la empresa adjudicataria considere necesario para satisfacer, con garantías, todas y cada una de las fases antes descritas y los productos y servicios indicados.

Los profesionales que sean responsables de la ejecución del trabajo deberán disponer de la cualificación y experiencia necesarias para que se lleven a cabo de forma satisfactoria los trabajos indicados y se alcancen los objetivos deseados, valorándose especialmente:

- Para la elaboración del libro blanco de la ciberseguridad en Navarra:
  - Conocimiento demostrable de los entornos de ciberseguridad regional y global.
  - Haber participado en proyectos de similar naturaleza al objeto del presente pliego.

- Para el desarrollo del cuadro de mando y observatorio sectorial de la ciberseguridad en Navarra:
  - Jefatura de proyecto con experiencia de al menos 10 años en desarrollo de herramientas similares.
  - Desarrollador/es e integrador/es con al menos 5 años de experiencia en desarrolló de cuadros de mando en Power BI.
  - Desarrollador/es con al menos 5 años de experiencia en el desarrollo de integración de datos de Power BI con otras herramientas como por ejemplo CMS o SharePoint.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

El personal asignado al contrato dependerá exclusivamente de la empresa adjudicataria. En ningún supuesto podrá considerarse con relación laboral, contractual, funcionarial o de naturaleza alguna respecto del Gobierno de Navarra, NASERTIC, y/o sociedades participadas por los mismos, tanto durante la vigencia del contrato como al término de este.

6 DIRECCIÓN Y CONTROL DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto en NASERTIC, la completa supervisión y dirección de los trabajos, proponer las modificaciones convenientes o, en su caso, proponer la suspensión de los mismos si existiese causa suficientemente motivada.

Para la supervisión de la marcha de los trabajos, NavCC indicará al comienzo del proyecto, la persona que ostentará la Dirección de Proyecto en NASERTIC y la composición de miembros del Equipo Director. Las funciones de este equipo en relación con el presente pliego serán:

- Velar por el adecuado cumplimiento de los servicios contratados.
- Independientemente de las reuniones ya establecidas en el Plan de Proyecto, la Dirección de Proyecto podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento del calendario del proyecto, así como la correcta consecución de los objetivos propuestos. El adjudicatario será responsable de la redacción y distribución de los informes de seguimiento y las correspondientes actas de reunión.
- Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Equipo Director de Proyecto, se marcarán desde el lanzamiento las directrices de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del adjudicatario.
- Durante el desarrollo del proyecto se podrán solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como evitar y reducir riesgos de desviación (en plazo y/o alcance) a lo largo del proyecto.

En las reuniones periódicas se evaluarán todas aquellas incidencias habidas que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio de la Dirección del Proyecto, tales incidencias fueran imputables al adjudicatario, por falta de responsabilidad, incompetencia, desidia u otras causas de índole similar, podría la facturación resultante quedar minorada por el importe que corresponda de acuerdo a las penalizaciones establecidas en el Pliego de Cláusulas Administrativas Particulares.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua

7 OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por la Dirección de Proyecto, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Así mismo, el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por la Dirección de Proyecto, quién se compromete a citar con la debida antelación al personal del adjudicatario.

Como parte de las tareas objeto del contrato, el adjudicatario se compromete a generar la documentación de los trabajos realizados, de acuerdo con los criterios que establezca en cada caso la Dirección de Proyecto. Toda la documentación generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva de NASERTIC sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de NASERTIC, que la concederá, en su caso y con expresión del fin, previa petición formal del adjudicatario.

En este sentido, el adjudicatario deberá informar a la Dirección de Proyecto sobre distintos aspectos relacionados con el funcionamiento y la calidad de los servicios prestados. Entre ellos será necesario presentar un informe en el formato y con la periodicidad que defina la Dirección de Proyecto, de cumplimiento de los servicios.

El adjudicatario proporcionará, sin coste adicional para la Sociedad, una copia en soporte digital con toda la documentación generada durante la prestación de los servicios objeto del contrato.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua