

Número de expediente: 2025012 Armonizado

Objeto de la contratación: Mesas vascas de ciberseguridad – Servicios de consultoría de apoyo para la realización de diagnóstico de situación y necesidades en materia de ciberseguridad de las empresas de los diferentes sectores económicos y cadenas de valor de Euskadi, que permitan diseñar nuevos programas y servicios dirigidos a las empresas, así como a su evaluación y seguimiento, dentro del marco del Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU

Documento: Pliego de prescripciones técnicas.

1. INTRODUCCIÓN

La “Estrategia para la Transformación Digital de Euskadi 2025” es la herramienta básica del Gobierno Vasco para impulsar la transformación digital de Euskadi, y fue aprobada por el Consejo de Gobierno en fecha 30 de marzo de 2021.

Dicha estrategia, liderada por el Departamento de Industria, Transición Energética y Sostenibilidad del Gobierno Vasco, acompañará con un apoyo sinérgico, proactivo y coordinado de todos los agentes involucrados, el reto que impone un nuevo modelo de transformación digital.

Las tecnologías digitales están destinadas a impulsar el crecimiento presente y futuro de todas las organizaciones, así como a aumentar la demanda de nuevas funciones, conjuntos de aptitudes y perfiles laborales. Las empresas esperan reestructurar su fuerza de trabajo en respuesta a la creciente automatización, reduciendo los perfiles más tradicionales y sustituyéndolos por otros más tecnológicos o ampliando la subcontratación para trabajos especializados.

La ETDE2025 se estructura en tres dimensiones que permiten definir los elementos sobre los que el Gobierno Vasco ha puesto su foco y sus prioridades durante el periodo de vigencia de la Estrategia. Estas dimensiones son las **palancas tecnológicas**, los **habilitadores de apoyo** y los **ámbitos de aplicación**. Estas tres dimensiones no actúan de forma aislada sino como un sistema y debe contemplarse desde la perspectiva de la generación de valor para Euskadi. A partir de ahí, la selección de las palancas tecnológicas se ha llevado a cabo teniendo en cuenta el papel disruptivo que están llamadas a tener a corto, medio y largo plazo en los retos que se plantean en las tres transiciones. Los habilitadores se conforman como los medios, canales o capacidades que favorecen y aceleran el despliegue de las tecnologías digitales.

Una de estas “palancas tecnológicas” identificadas es la “CIBERSEGURIDAD Y CONFIANZA DIGITAL”.



Relacionado con esto último, en los últimos años, la sociedad en general y el entorno empresarial en particular han experimentado una profunda transformación tecnológica, impulsando el desarrollo y la optimización de procesos y servicios en las organizaciones. Este avance no solo ha revolucionado las dinámicas empresariales, sino que también ha incrementado significativamente su dependencia de la tecnología. Como consecuencia, la hiperconectividad derivada de esta dependencia se ha convertido en un factor clave en el aumento de la cibercriminalidad, elevando los riesgos en materia de ciberseguridad. Estos riesgos no solo afectan la integridad, confidencialidad y disponibilidad de la información, sino que también impactan directamente en la prestación de servicios de las diferentes entidades que operan en los diferentes estados.

De esta manera, en los últimos años, el aumento de ciberamenazas ha sido una constante tanto en el ámbito empresarial como en el sector público, afectando de manera indiscriminada a todo tipo de organizaciones, independientemente de su tamaño, sector o condición. Tanto las administraciones públicas como las empresas privadas se encuentran en el punto de mira de estos ataques. La materialización de tales amenazas puede tener consecuencias devastadoras para las empresas, incluyendo pérdidas económicas significativas, un daño reputacional que podría comprometer sus relaciones con clientes y proveedores, así como sanciones regulatorias. Todo esto repercute directamente en la competitividad de las organizaciones, dificultando su capacidad para operar de manera eficiente en sus respectivos mercados.

La ciberseguridad por la tanto resulta a día de hoy un aspecto de vital relevancia para las empresas y los diferentes sectores económicos, hasta el punto de que en algunos casos puedes significar un elemento diferenciador o factor clave en sus relaciones empresariales y actividad económica, erigiéndose como un elemento fundamental para la competitividad de las mismas. En este contexto, y desde una perspectiva de promoción económica, desde SPRI se trata de promocionar la ciberseguridad con el objetivo de que las empresas de Euskadi puedan mejorar sus capacidades en esta materia, para que se puedan mostrar como una opción segura y confiable en sus respectivos mercados y con sus clientes, contribuyendo de esta manera a una mejora de su competitividad.

Bajo esta perspectiva, si bien es verdad que las ciberamenazas ponen el foco de forma indiscriminada en cualquier tipo de entidad o colectivo, la naturaleza de estos entornos hace que el punto de partida, así como las necesidades entre unos y otros difieran, en algunos casos, considerablemente. De esta manera, con carácter general el nivel de madurez en términos de ciberseguridad tiende a no ser el mismo entre diversos sectores, al mismo tiempo que existen otra serie de cuestiones como la regulación, la cultura de la ciberseguridad, la frecuencia y las diversas formas de ataque, la cadena de suministro, las necesidades en cuanto a productos y soluciones tecnológicas, que pueden variar significativamente entre unos sectores económicos y otros. Por poner un ejemplo, los sectores más regulados y con mayor impacto económico tienden a estar mejor preparados y a poseer un nivel más alto en materia de ciberseguridad, protección y resiliencia.

Por estos motivos, desde una visión de desarrollo económico, desde SPRI se reconoce la necesidad de conocer mejor cual es la naturaleza y situación de estos entornos y sectores económicos de Euskadi, al mismo tiempo que identificar cuáles son sus necesidades en materia de ciberseguridad, al objeto de mejorar en el diseño y personalización de instrumentos de apoyo a la promoción económica para las empresas para que puedan dar respuesta a los desafíos de los diferentes sectores económicos, así como para tratar de contribuir a una mejor definición de la oferta en ciberseguridad en el territorio, favoreciendo al desarrollo y crecimiento del sector y del tejido empresarial de ciberseguridad de Euskadi. De esta forma, los servicios de apoyo objeto de la presente contratación centrarán el foco en contribuir a la realización de una serie de diagnósticos en cuanto a situación y necesidades en materia de ciberseguridad para los diferentes sectores económicos y cadenas de valor vinculadas a las 17 ODCs (Organizaciones Dinamizadores de Clusters) existentes en Euskadi, con las que SPRI tiene relación y colaboración activa. Estos diagnósticos en cuanto a situación y necesidades permitirán avanzar en la definición de nuevas políticas públicas, así como en el diseño de nuevos programas y servicios con una orientación más sectorial, al mismo tiempo que customizada a las necesidades reales de las empresas de cada uno de estos sectores económicos. Adicionalmente, los servicios de consultoría de apoyo objeto de la presente contratación, servirán para realizar una evaluación y seguimiento de los diferentes programas y servicios que se estuvieran impulsando o se quisieran impulsar desde el departamento de industria, transición energética y sostenibilidad del Gobierno Vasco, a través de SPRI. Así pues, los diagnósticos a realizar pondrán el foco en una serie de ámbitos objeto de estudio tales como el entorno regulatorio y normativo, infraestructuras y tecnologías necesarias, talento y capacitación, cultura de ciberseguridad y concienciación, inversión y recursos económicos, o la innovación y cooperación entre otros.

Este servicio está enmarcado dentro del CONVENIO DE COLABORACIÓN EN EL ÁMBITO DE LA CONVOCATORIA RETECH CIBERSEGURIDAD (REDES TERRITORIALES DE ESPECIALIZACIÓN TECNOLÓGICA) DE LA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL formalizado en noviembre del 2023 entre otros por SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL e INCIBE (S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A.)

Los objetivos estratégicos que se marcaron dentro el proyecto presentado por el Gobierno Vasco a esta convocatoria, y denominado PROYECTO RED-ARGOS, son, entre otros, los siguientes:

- Fortalecer la industria de ciberseguridad con un ecosistema de innovación público-privado a través del desarrollo de actividades de I+D+i para la experimentación y la generación de una red de infraestructuras lógicas o físicas de conocimiento distribuido que ofrezca complementariedad, la transferencia a empresas, la especialización tecnológica, la llegada al mercado de soluciones y la creación de productos en toda la cadena de valor.

- Mejorar la permeabilidad de la ciberseguridad a todos los sectores económicos, para así aumentar su adopción global.
- Promover, hacer crecer y consolidar la colaboración interregional, apoyándose en las fortalezas de cada comunidad autónoma participante en la propuesta para conseguir un mayor efecto tractor en el campo de la ciberseguridad como oportunidad económica, profesional y empresarial.
- Mejorar las capacidades con las que ya se cuenta a nivel regional, incorporando nuevas infraestructuras, equipamientos y recursos que permitan su especialización.
- Incrementar la adopción global de medidas de ciberseguridad, desde el diseño y en el resto de etapas. Desarrollo de nuevas soluciones.
- Atraer y generar talento con el desarrollo de estrategias de captación y capacitación en ciberseguridad, tanto a nivel de oferta como de demanda a través de planes de formación e itinerarios especializados con competencias y perfiles profesionales, que aceleren el desarrollo de la Ciberseguridad.
- Impulsar el emprendimiento en ciberseguridad, y la aceleración especialmente de las PYMEs, con una mejor visibilidad y llegada al mercado.

A este respecto, dentro del marco del RETECH Ciberseguridad, a día de hoy ya se han definido una serie de iniciativas (programas y servicios) de apoyo para las empresas de Euskadi con el objetivo de mejorar sus capacidades en materia de ciberseguridad, favoreciendo al desarrollo y fortalecimiento del sector y del tejido empresarial de ciberseguridad en el territorio. En este sentido, los estudios objeto de la presente contratación, servirán para avanzar en el rediseño de estos instrumentos, así como para la definición de nuevas iniciativas de apoyo para las empresas en materia de ciberseguridad. Concretamente, el conocer la situación y necesidades en materia de ciberseguridad de los diferentes sectores económicos del territorio, permitirá proporcionar, así como otorgar una orientación más sectorial a algunos de estos instrumentos, garantizando un mejor aprovechamiento de los mismos por parte de las empresas, al mismo tiempo que resultando en escenarios lo suficientemente representativos para que las empresas de los diferentes sectores económicos se puedan sentir reflejadas, y por lo tanto beneficiadas. Esto último puede resultar diferencial, ya que como se ha mencionado anteriormente, no todos los sectores económicos enfrentan los mismos desafíos y amenazas en el campo de la ciberseguridad.

A continuación se presentan algunas de las iniciativas de apoyo para las empresas que, sin ánimo limitativo ni exhaustivo, se prevé puedan ser puestas en marcha próximamente, dentro de la convocatoria RETECH Ciberseguridad (Fondos NextGenerationEU).

Iniciativa	Presupuesto
Programa de Ayudas "Servicios SOC y Certificaciones en Ciberseguridad"	3.696.389,00 €
Programa de ayudas "Ciberseguridad Empresarial"	4.500.000,00 €
Programa de ayudas "Competencias Digitales en Ciberseguridad"	2.000.000,00 €
Simulacros de incidentes de ciberseguridad en Equipos Directivos/Responsables	3.500.000,00 €
Total	13.696.389,00 €

2. OBJETO DE LA CONTRATACIÓN

La presente licitación tiene por objeto la contratación de servicios de consultoría de apoyo para la realización de diagnósticos en cuanto a situación y necesidades en materia de ciberseguridad de las empresas de los diferentes sectores económicos y cadenas de valor vinculadas a las 17 ODCs (Organizaciones Dinamizadores de Clústeres) existentes en Euskadi, que permitan diseñar nuevos programas y servicios dirigidos a las empresas, así como a su evaluación y seguimiento.

En este sentido, al objetivo de facilitar este análisis y de cara a favorecer a la consecución de los objetivos y garantizar el grado de alineamiento con las orientaciones sectoriales que establece la convocatoria RETECH Ciberseguridad (Redes Territoriales de Especialización Tecnológica), desde SPRI se propone agrupar los diversos sectores económicos objeto de este estudio en diferentes lotes. De esta manera la presente contratación constará de 4 lotes independientes que se corresponderán con los diferentes sectores económicos objeto de este contrato, y que a su vez estarán relacionados con las 17 ODCs (Organizaciones Dinamizadores de Clústeres) existentes en Euskadi.

- **Lote 1.** Aeronáutica y Espacio; Automoción; Siderurgia; Fundición y Forja.
- **Lote 2.** Máquina-Herramienta; Equipos Ferroviarios; Industrias Marítimas.
- **Lote 3.** Energía; Medio ambiente; Papel, Alimentación.
- **Lote 4.** Transportes, movilidad y Logística; Construcción; Equipamiento, diseño y madera; Finanzas e inversión.

Las actividades objeto de la presente contratación y de cada uno de los lotes objeto de la misma se llevarán a cabo en el ámbito de la CAE.

3. OBJETIVOS Y DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR

3.1. Objetivo

La presente licitación tiene como finalidad la contratación de servicios de consultoría de apoyo para la realización de diagnósticos en cuanto a la situación y necesidades en materia de ciberseguridad en los diferentes sectores económicos y cadenas de valor vinculadas a las 17 ODCs (Organizaciones Dinamizadores de Clústeres) existentes en Euskadi, que permitan diseñar nuevos programas y servicios dirigidos a las empresas, así como a su evaluación y seguimiento. Se espera que estos diagnósticos incluyan entre otros, un análisis de la situación actual del sector en materia de ciberseguridad, principales necesidades, retos presentes y futuros, actores clave, así como posibles planes de acción con una serie de iniciativas dirigidas a contribuir a mejorar las capacidades de dichos sectores o cadenas de valor en esta materia, por medio del desarrollo y fortalecimiento del sector de la ciberseguridad en Euskadi. Cabe señalar,

que los estudios objeto de la presente contratación se realizarán desde una perspectiva y con una finalidad de promoción o desarrollo económico, poniendo el foco en la mejora de la competitividad de las empresas que operan en estos sectores por medio de la mejora de su nivel de ciberseguridad, de protección y de resiliencia.

De esta manera, las actividades objeto de la presente contratación deberán de favorecer, entre otros, a la consecución de los siguientes objetivos específicos:

- Mejora en cuanto a la definición de nuevas políticas públicas relacionadas con la promoción económica. Disponer de mayor contexto de cara a diseñar y lanzar nuevas iniciativas de apoyo para las empresas para mejorar sus capacidades en materia de ciberseguridad, así como para el desarrollo del sector y del tejido empresarial de ciberseguridad de Euskadi.
- Evaluación y seguimiento de las iniciativas de apoyo para las empresas para mejorar sus capacidades en materia de ciberseguridad, que se estuvieran impulsando o se quisieran impulsar desde el departamento de industria, transición energética y sostenibilidad del Gobierno Vasco, a través de SPRI.
- Mejora del conocimiento en lo que se refiere a la demanda. Conocer necesidades concretas de las empresas de Euskadi en materia de ciberseguridad, normativa que les aplica, principales amenazas que enfrentan, soluciones tecnológicas y servicios que pudieran requerir, etc.
- Generación de demanda. Identificación de actores clave en los diferentes sectores económicos de Euskadi con casos de uso ejemplarizantes para su visibilización.
- Mejora en cuanto a la definición de la oferta. Generación de nuevas empresas y nuevos modelos de negocio. Definición y desarrollo de nuevos productos y nuevos servicios. Certificaciones y alianzas entre empresas del ámbito de la ciberseguridad.
- Extender una cultura de ciberseguridad entre las empresas.
- Programas de formación específicos. Identificación de itinerarios de formación y capacitación específicos para los diferentes sectores económicos de Euskadi.
- Fomento de la innovación, la I+D y el emprendimiento.
- Alianzas y colaboraciones entre agentes para potenciar la ciberseguridad como elemento estratégico dentro del ámbito empresarial.

En este sentido, y de cara a avanzar en la consecución de estos objetivos, a lo largo de la ejecución de la presente contratación se abordarán las siguientes fases. Estas fases, así como las actividades a desarrollar descritas en el apartado siguiente serán las mismas para todos y cada uno de los lotes anteriormente mencionados.

Fase 1: Definición de Objetivos y Planificación Inicial.

- Definir el Propósito y Objetivos de estos diagnósticos.
- Definición de ámbitos objeto de estudio (Normativo, Infraestructuras, Talento, Necesidades de inversión, etc).
- Identificación de actores claves y grupos de interés.

- Caracterización de los diferentes sectores objeto de la presente licitación.
- Definición de metodología y fuentes de datos.

Fase 2: Análisis y Diagnóstico.

- Recopilación de información y contraste.
- Categorización y análisis de información.
- Determinación de la situación para los ámbitos objeto de estudio.
- Identificación de necesidades y oportunidades dentro de los ámbitos objeto de estudio.
- Identificación de capacidades en materia de ciberseguridad en Euskadi en los ámbitos objeto de estudio.
- Comparativas con otros países/regiones que sirvan como referencia en materia de ciberseguridad para los diferentes sectores económicos de Euskadi y benchmarking de iniciativas en los ámbitos objeto de estudio.

Fase 3: Estrategia y Líneas de Acción.

- Estrategia con líneas de acción para el fortalecimiento de la ciberseguridad en los diferentes sectores económicos de Euskadi desde una perspectiva de promoción económica.
- Identificación y definición de iniciativas dirigidas al impulso y promoción de la ciberseguridad para las empresas por parte de las instituciones públicas desde una perspectiva de promoción económica.
- Seguimiento y evaluación de estas iniciativas.
- Identificación de alianzas estratégicas que favorezcan al fortalecimiento de la ciberseguridad en los diferentes sectores económicos de Euskadi.
- Informes de situación y de estrategia.
- Apoyo técnico a las personas de SPRI designadas por la persona responsable de la presente contratación en lo relacionado a las líneas de acción, así como las iniciativas de apoyo para las empresas en materia de ciberseguridad que pudieran surgir como resultado de la presente contratación.

Para abordar estas fases, así como algunas de las actividades a desarrollar descritas en el siguiente apartado, será necesario involucrar a determinados agentes del territorio que pudieran tener conocimiento en lo relativo a estos sectores económicos, así como en los ámbitos objeto de estudio identificados, tales como el ámbito normativo, infraestructuras, talento o necesidades de inversión, entre otros. De esta manera, en la parte de la demanda, al objeto de poder recabar información en cuanto a situación y necesidades, se espera poder disponer de la visión de las diferentes ODCs (Organizaciones Dinamizadores de Clústeres) que existen en Euskadi (se pueden encontrar en el siguiente enlace: www.spri.eus/es/ris3-euskadi/politica-de-clusters/), y que vienen a representar diferentes sectores económicos y cadenas de valor del territorio, así como la perspectiva de determinadas empresas y profesionales que pudieran tener un peso relevante o un papel clave en cada uno de los diferentes sectores económicos objeto de la presente licitación.

Además de eso, se deberá de implicar a otra serie de agentes o agrupaciones empresariales relevantes que pudieran tener conocimiento sobre el grado de madurez en ciberseguridad de estos sectores económicos, así como a instituciones públicas que pudieran operar en estos ámbitos o que desarrollasen su actividad dentro del campo de la ciberseguridad.

Por último, a lo largo de las diferentes fases, será necesario conocer y contar con determinados agentes que conforman el ecosistema tecnológico y de ciberseguridad de Euskadi, al objeto de tratar de identificar cuáles son las capacidades del territorio en materia de ciberseguridad en determinados ámbitos específicos. También resultará necesario que las empresas adjudicatarias posean conocimiento sobre el tejido empresarial de ciberseguridad del territorio.

3.2. Actividades objeto del contrato

Las actividades objeto de este contrato serán las mismas para cada uno de los lotes y se corresponderán con cada una de las fases previamente mencionadas. De esta forma en cada una de estas fases, la empresa adjudicataria deberá de realizar las siguientes actividades y tareas:

Fase 1: Definición de Objetivos y Planificación Inicial.

- Definición de los objetivos e identificación de los ámbitos que serán objeto de estudio para los diferentes sectores económicos y cadenas de valor vinculadas a las 17 ODCs (Organizaciones Dinamizadores de Clústeres) existentes en Euskadi.
- Labores de prospección en cuanto a ejercicios de naturaleza similar llevados a cabo por parte de otras instituciones públicas o cualquier otro tipo de entidad.
- Definición de una metodología para la realización de los diagnósticos de situación y necesidades en materia de ciberseguridad para los diferentes sectores económicos objeto de cada uno de los lotes.
- Identificación de actores clave, así de grupos de interés que pudieran resultar relevantes para la realización de estos diagnósticos.
- Labores de categorización y definición de taxonomía dirigidas a caracterizar los diferentes sectores económicos objeto de estudio, tratando de representar los diferentes eslabones que representan las cadenas de valor presentes en cada uno de los sectores económicos.
- Definición de un marco, así como definición o utilización de herramientas dirigidas a determinar el grado o nivel de madurez de ciberseguridad de los diferentes sectores económicos objeto de los diferentes lotes, teniendo en consideración los ámbitos objeto de estudio anteriormente definidos.
- Definición de una planificación que incluya las diferentes acciones que se van a llevar en las siguientes fases, así como posibles hitos y entregables, al objeto de garantizar que los diagnósticos se alinean con los objetivos y los plazos temporales que establece la convocatoria RETECH Ciberseguridad.

- Definición de estructura en cuanto a los entregables objeto de la presente contratación.

Fase 2: Análisis y Diagnóstico.

- Labores de contraste con los actores y grupos de interés identificados en la Fase 1, así como recopilación de tanta información como sea necesaria al objeto de determinar la situación y necesidades en materia de ciberseguridad en los diferentes sectores económicos de Euskadi objeto de estudio.
- Labores dirigidas a la caracterización de los diferentes sectores económicos objeto de estudio.
- Labores de categorización y de análisis de la información recopilada, así como adaptación de la misma al objeto de poder disponibilizarla posteriormente en forma de los entregables definidos dentro del marco de la presente contratación.
- Actividades, así como aplicación de metodología y herramientas dirigidas a determinar la situación en materia de ciberseguridad en los ámbitos objeto del estudio para los sectores económicos de cada uno de los lotes anteriormente descritos.
- Actividades dirigidas a identificar las necesidades en materia de ciberseguridad en los ámbitos objeto del estudio, así como establecer un modelo que conforme a unos criterios determinados y adecuados permita trabajar en una priorización u ordenación en cuanto a dichas necesidades. (Ej: priorización en función del impacto para la competitividad de estos sectores económicos).
- Análisis DAFO y GAP para cada uno de los sectores económicos objeto de cada uno de los lotes.
- Identificación de capacidades en materia de ciberseguridad en Euskadi en los ámbitos objeto de estudio, así como trabajar, en su caso, en una categorización de las mismas.
- Identificación de modelos y buenas prácticas en cuanto a iniciativas, dentro de los ámbitos objeto de estudio, promovidas por parte de otra serie de instituciones o entidades de otros países/regiones que sirvan como referencia.

Fase 3: Estrategia y Líneas de Acción.

- Elaboración de informes de situación y necesidades en materia de ciberseguridad para los diferentes sectores económicos objeto de este estudio.
- Elaboración de estrategia con líneas de acción para el fortalecimiento de la ciberseguridad en los diferentes sectores económicos de Euskadi objeto de este estudio desde una perspectiva de promoción económica.
- Identificación de planes o estrategias promovidos por otras instituciones públicas dentro del marco de las temáticas de la presente contratación (ciberseguridad, promoción económica, tecnología, sectores económicos vinculados a las ODCs de Euskadi, etc), así como tantas labores como fueran

pertinentes, de cara a garantizar el alineamiento entre la estrategia y las líneas de acción definidas en la presente contratación y las mismas.

- Labores dirigidas a la identificación y definición de iniciativas dirigidas al impulso y promoción de la ciberseguridad para las empresas por parte de las instituciones públicas desde una perspectiva de promoción económica.
- Seguimiento y evaluación de estas iniciativas.
- Realización de reuniones con otros agentes dirigidos a presentar los resultados objeto de los diagnósticos realizados.
- Acompañamiento en cuanto la participación en eventos enfocados a dar a conocer los resultados objeto de los diagnósticos realizados.
- Labores de apoyo y asesoramiento técnico a las personas designadas por SPRI como responsables de la presente contratación dentro de los ámbitos objeto de la presente contratación.
- Elaboración de entregables y material de apoyo dirigido a presentar los resultados objeto de los diagnósticos realizados.

Sin perjuicio de que la planificación de estas fases se presente y valide en las reuniones de lanzamiento de los servicios sobre la base de la propuesta presentada por la adjudicataria, a continuación se presenta de manera tentativa una aproximación en cuanto a planificación, al objeto de tratar de dar a conocer a las potenciales empresas adjudicatarias de la presente licitación, el grado de dedicación de cada una de las fases, así como el horizonte temporal inicialmente planteado para los diagnósticos objeto del contrato.

Fases	M1	M2	M3	M4	M5	M6	M7
Fase 1: Definición de Objetivos y Planificación Inicial.							
Fase 2: Análisis y Diagnóstico.							
Fase 3: Estrategia y Líneas de Acción.							

3.3. Entregables

Dentro del marco de la presente contratación SPRI precisará la elaboración de una serie de entregables que garanticen el cumplimiento de los objetivos del proyecto, al mismo tiempo que permitan dar a conocer los resultados objeto de los diagnósticos realizados. De esta manera, las empresas adjudicatarias deberán de elaborar al menos un informe en el que se presente la información de los diagnósticos realizados, para cada uno de los sectores económicos objeto de su lote. Estos informes se elaborarán tanto en versión Word como en versión PowerPoint, así como en las dos lenguas oficiales de la Comunidad Autónoma de Euskadi (asumiendo la contratista la responsabilidad y coste de la traducción), y aunque la estructura se definirá y validará entre las dos partes en las reuniones de lanzamiento de los servicios sobre la base de la oferta adjudicataria, los informes deberán de contener al menos los siguientes apartados: i) Introducción, ii) Contexto y Necesidad, iii) Objetivos del informe, iv) Metodología, v) Ámbitos objeto de

estudio, vi) Resultados, vii) Conclusiones y perspectivas futuras, viii) Estrategia y Plan de Acción.

A la finalización del M6, coincidiendo con el inicio de la “Fase 3: Estrategia y Líneas de Acción”, las empresas adjudicatarias deberán de elaborar una primera versión de estos entregables, las cuales serán validadas por la persona responsable del contrato.

Del mismo modo, las empresas adjudicatarias deberán entregar la versión final de estos entregables a la finalización del M7, las cuales se darán por cerradas una vez cuente con el visto bueno y validación de la persona responsable del contrato.

Adicionalmente, para algunos de los ámbitos objeto de estudio, SPRI podrá requerir la elaboración de otra serie de informes dirigidos a presentar un análisis más pormenorizado en lo relativo a cada uno de estos ámbitos. Del mismo modo, algunos de estos informes o documentos podrán ser requeridos en formatos específicos al objeto de utilizarlos para el desarrollo y elaboración de cuadros de mandos a partir de herramientas de Business Intelligence.

3.4. Dimensionamiento del servicio

En las reuniones de lanzamiento de los servicios, que serán individuales para cada uno de los lotes, las adjudicatarias deberán presentar a SPRI el equipo de trabajo asignado al proyecto, indicando una previsión en términos de dedicación para cada uno de los perfiles expuestos para toda la vigencia del contrato sobre la base de lo propuesto en la oferta. Asimismo, será responsabilidad del/la jefe/a de proyecto de cada empresa adjudicataria comunicar a SPRI el rol específico que desempeñará cada integrante del equipo a lo largo del contrato, así como el perfil profesional al que se le vincula (por ejemplo: Consultor/a Especialista, Consultor/a de Apoyo, ...), conforme a los perfiles profesionales descritos en el Pliego de Cláusulas Administrativas Particulares.

Las empresas adjudicatarias deberán prestar sus servicios utilizando como mínimo el equipo y las personas especificadas en su oferta. Cualquier sustitución de estas personas estará sujeta a lo establecido en el Pliego de Condiciones Administrativas Particulares.

Del mismo modo, las personas del equipo de trabajo del proyecto deberán de garantizar disponibilidad según el cronograma que se defina en la reunión de lanzamiento sobre la base de la propuesta adjudicataria, el cual deberá de ser aprobado por ambas partes (contratistas y adjudicataria). Del mismo modo, los consultores deberán asistir a todas las reuniones, talleres, presentación y comités relacionados con el proyecto, ya sea de forma presencial o remota, según lo que determine SPRI sobre la base de las necesidades en cada caso. En caso de periodos de indisponibilidad, ausencia planificada o imprevista de alguna de las personas del equipo de trabajo, la adjudicataria deberá de avisar con la suficiente antelación de cara a poder garantizar la continuidad del proyecto

sin afectar a los plazos, hitos o entregables definidos en la reunión de lanzamiento del proyecto.

Adicionalmente, en las reuniones de lanzamiento de los servicios, las empresas adjudicatarias también deberán de presentar, sobre la base de lo propuesto en sus ofertas, una planificación para las fases y para la realización de las actividades objeto de la presente contratación. En dicha reunión, se fijarán con carácter definitivo, entre otras, las siguientes cuestiones: i) Alcance, ii) Objetivos, iii) Resultados esperados y entregables, iv) Metodología, v) Fases e Hitos, vi) Plazos y deadlines, vii) Equipo de Trabajo, viii) Mecanismos de Seguimiento, ix) Canales de comunicación.

Una vez presentada esta información, en el plazo de 10 días hábiles, la persona responsable del contrato por parte de SPRI analizará las propuestas y, en su caso, procederá a validar las propuestas dando por iniciado los servicios correspondientes a cada uno de los lotes.

Los servicios se prestarán en lengua castellana o euskera, a decisión de la parte contratante. En el supuesto de que las personas de las partes contratadas, dedicadas a estos servicios, no dispusieran de conocimientos suficientes de euskera, las contratistas deberá garantizar, a través de cualquier otro medio más adecuado, la canalización, a su cargo, de los servicios en dichas lenguas.

Se estima con carácter orientativo y en ningún caso vinculante un volumen de trabajo a lo largo de la presente contratación para cada uno de los lotes de entre 250-300 jornadas, bajo la siguiente estimación de dedicaciones para los perfiles requeridos respecto al total del proyecto:

- Consultor/a Jefe del proyecto (20%)
- Consultor/a experto/a especialista (40%)
- Asesor/a jurídico (10%)
- Consultor/a técnico/a de apoyo (30%)

A efectos aclaratorios, se considerará como jornada de trabajo la media de 8 horas por día.

4. EQUIPO DE TRABAJO Y PERFILES PROFESIONALES REQUERIDOS

El equipo de trabajo que las licitadoras oferten en su propuesta técnica deberá incluir personal cualificado y estar compuesto por técnicos especialistas ya sea en ciberseguridad, en consultoría estratégica, así como en derecho relacionado con las TICs

o la ciberseguridad. En particular, el equipo de trabajo que se proponga deberá cumplir con, al menos, las siguientes condiciones:

- a- Designación de una persona (consultor/a jefe/a del proyecto) que ejerza como responsable general de los Servicios a prestar e interlocutor con la persona responsable en SPRI, con conocimiento y experiencia suficientes en labores de naturaleza similar a la del objeto del presente pliego, esto es, en el ámbito de la consultoría tecnológica o de ciberseguridad, así como en consultoría estratégica.
- b- Para la ejecución de las labores descritas en el apartado 3º anterior, además de la persona que ejerza como consultor/a jefe/a de proyecto, se estima necesario, por cada adjudicatario, un equipo adicional mínimo de 3 personas (1 consultor/a experto/a especialista, 1 consultor/a técnico/a de apoyo y 1 asesor/a jurídico) con experiencia en el ámbito de la consultoría en ciberseguridad, consultoría estratégica, así como en derecho relacionado con las TICs o la ciberseguridad, tal y como se especifica en el cuadro descrito en el siguiente apartado.

Los trabajos desarrollados por el equipo del adjudicatario serán supervisados directamente por la persona responsable del contrato en SPRI.

SPRI podrá sugerir a la contratista, que se compromete a valorarlo, la incorporación de personas adicionales a los servicios, en función de las necesidades puntuales, siempre que sus perfiles sean similares a los de las personas propuestas en el equipo de trabajo.

En cualquier caso, el equipo de trabajo deberá estar compuesto, al menos, de los siguientes perfiles profesionales:

- Una persona, con formación superior en Ingeniería Industrial, Ingeniería Informática, Ingeniería de Telecomunicaciones, Física, Matemáticas o equivalentes, con formación específica en Ciberseguridad o en ámbito de las TICs, que ejerza como consultor/a jefe/a del proyecto e interlocutor principal con SPRI.
- Una persona con formación superior en Ingeniería Industrial, Ingeniería Informática, Ingeniería de Telecomunicaciones, Física, Matemáticas, o similares, con formación específica en Ciberseguridad o en ámbito de las TICs, que ejerza como consultor/a experto/a especialista.
- Una persona, con titulación académica de licenciatura o graduado/a en Derecho, que ejerza como asesor/a jurídico.
- Una persona, con titulación académica de licenciatura o graduado/a, que ejerza como consultor/a técnico/a de apoyo.

Los miembros del equipo propuesto deberán disponer de la siguiente experiencia mínima y cumplir con los roles a continuación detallados:

Perfil profesional	Experiencia mínima requerida
Consultor/a Jefe/a del proyecto	Más de 10 años de experiencia en consultoría relacionada con planes estratégicos, así como con proyectos dentro del ámbito de la ciberseguridad o las TICs.
Consultor/a experto/a especialista	Más de 5 años de experiencia en consultoría relacionada con planes estratégicos, así como con proyectos dentro del ámbito de la ciberseguridad o las TICs.
Asesor/a jurídico	Más de 5 años de experiencia en asesoramiento jurídico en proyectos relacionados con derecho de las TICs o la ciberseguridad.
Consultor/a técnico/a de apoyo	Más de 2 años en consultoría relacionada con planes estratégicos, así como con proyectos dentro del ámbito de la ciberseguridad o las TICs.

El equipo mínimo se entenderá sin perjuicio de la obligación de las empresas adjudicatarias de destinar el personal que sea necesario para la correcta ejecución del contrato y cumplir con las condiciones generales y específicas en cuanto a competencia técnica y profesional contenidas en la legislación vigente y requeridas en el presente Pliego, todo ello por cuanto los medios humanos constituyen un factor determinante en la calidad del servicio. Las personas que durante el período de duración de contrato resulten precisas para el desarrollo del mismo deberán cumplir los requisitos indicados según el perfil al que se adscriban.

5. SUPERVISIÓN Y CONTROL DEL SERVICIO

Los servicios a prestar serán supervisados por el Área de Transformación Digital de SPRI, y en particular por la persona responsable del contrato, que podrá pedir las explicaciones e informaciones que considere oportunas al objeto de verificar el correcto desarrollo de los trabajos contratados.

5.1. SUPERVISIÓN

Será responsabilidad de los jefes/as de proyecto de las adjudicatarias la supervisión de las diferentes actividades, servicios, entregables proporcionados a SPRI a lo largo de toda la duración del contrato, al objeto de garantizar que todas las fases del proyecto se lleven a cabo de manera exitosa y conforme a los objetivos y requisitos establecidos en la reunión inicial del proyecto.

De esta manera, estas personas deberán de supervisar, entre otras cuestiones, que el proyecto se encuentre alineado con los objetivos estratégicos de la empresa, que los recursos (humanos y tecnológicos) son adecuados y están disponibles según las necesidades del proyecto, que se esté cumpliendo con los plazos establecidos, que los diferentes entregables se desarrollan según las especificaciones acordadas y la calidad esperada, así como detectar cualquier desviación en el avance del proyecto, ya sea en tiempo, costo o alcance, que pudiera poner en riesgo el devenir del proyecto, y con el objetivo de poder definir y activar medidas correctivas cuando sea necesario.

5.2. MECANISMOS DE SEGUIMIENTO

Los equipos de trabajo estarán dirigidos por un/una jefe/a de proyecto, quien se encargará de la gestión y coordinación de las diferentes actividades objeto de la presente contratación, al mismo tiempo que será el/la interlocutor/a principal con el personal asignado por parte de SPRI como responsables del proyecto y del contrato.

Del mismo modo, las empresas adjudicatarias deberán de establecer y proporcionar todos aquellos mecanismos de control que permitan el seguimiento y la verificación de forma continuidad del cumplimiento de los objetivos establecidos en la reunión de lanzamiento del proyecto, tanto en plazos como en términos de calidad. Para ello se contemplan entre otros:

- Reuniones de seguimiento: se celebrarán reuniones periódicas destinadas a revisar el grado de cumplimiento y avance de las tareas planificadas, las reasignaciones de personal si fueran precisas, la validación de las programaciones de actividades a realizar, etc.
- Reuniones de seguimiento de ejecución de costes.

- Gestión de riesgos o bloqueos. Mantener un registro de los riesgos y bloqueos identificados, así como establecer un plan para su mitigación o desbloqueo.
- Informes de situación y progreso: con los que la adjudicataria comunicará a SPRI, el estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc.