Expediente nº: 2021018

Objeto de la contratación: Elaboración tercera edición del Libro blanco de ciberseguridad en Euskadi del Basque CyberSecurity Centre.

Documento: Pliego de prescripciones técnicas particulares.

Contenido

1. CONTEXTO 3
2. OBJETO DE LA CONTRATACIÓN 3
2.1. Antecedentes 3
2.2. Objeto 5
3. DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR 5
3.1. Consideraciones previas 5
3.2. Actividades objeto del contrato 5
3.2.1. Contextualización del ecosistema 5
3.2.2. Definicion de criterios de categorización de AGENTES 6
3.2.3. segmentación de los agentes del ecosistema de la ciberseguridad 7
3.3. Planificación de actividades y metodología 7
3.4. Equipo de trabajo 8
3.4.1. Composición 8
3.4.2. Perfiles adscritos al proyecto 8
3.5. Dirección y seguimiento de los trabajos 8
3.6. Obligaciones de información y documentación 9
3.7. Entregables 9

1. CONTEXTO

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca dentro de SPRI – Agencia Vasca de Desarrollo Empresarial (en adelante SPRI), entidad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco.

El BCSC, como unidad de SPRI, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico, Sostenibilidad y Medio Ambiente, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación. La actividad abarca proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de. Comité Permanente del BCSC.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

2. OBJETO DE LA CONTRATACIÓN

2.1. ANTECEDENTES

La Estrategia para la Transformación Digital de Euskadi 2025 (ETDE2025), la Estrategia de Fabricación Avanzada (Basque Industry 4.0), Líneas Estratégicas y Económicas básicas del PCTI Euskadi 2030 (PCTI Euskadi 2030) y la Estrategia Regional de Especialización Inteligente en Innovación (RIS3 Euskadi) establecen como línea de acción estratégica el impulso a la industria de la ciberseguridad en dos facetas. Por un lado, se promoverá el sector relacionado con esta actividad y, por otro, se fomentará su aplicación en la industria como habilitador clave de la competitividad. Los cuatro ejes anteriores apuestan por establecer mecanismos de impulso a la I+D+i, aprovechando el ecosistema e iniciativas público-privadas existentes, mejorando el acercamiento entre la oferta y la demanda, identificando prioridades de investigación, y de ese modo sirviendo de catalizador para un mejor posicionamiento de la industria vasca en el panorama de competitividad internacional.

El Plan de Impulso de la Economía Digital y de los Contenidos Digitales del Estado Español prevé el desarrollo de polos tecnológicos de gran impacto que atraigan la inversión extranjera directa y la búsqueda de los impulsos que hagan nacer, de forma espontánea, la concentración sectorial, de forma que su desarrollo sea sostenible y no dependa permanentemente del apoyo público a medio y largo plazo. En este sentido, en materia de ciberseguridad y confianza ya

existen algunas iniciativas público-privadas de referencia en la región.

Dadas las privilegiadas características de partida que se disponen en la Comunidad Autónoma de Euskadi, el Gobierno Vasco desea recoger todas estas capacidades en un estudio sectorial.

Primera edición del libro blanco de la ciberseguridad de Euskadi

Este estudio se realizó en 2018 y se encuentra publicado en el siguiente enlace: https://www.basquecybersecurity.eus/archivos/201902/bcsc_libro_blanco_v7.pdf

La primera edición del libro blanco de la ciberseguridad en Euskadi consistió en un análisis pormenorizado del sector de la ciberseguridad incluyendo aspectos clave como perspectivas y oportunidades del sector y el detalle de la situación actual de las organizaciones dedicadas a la ciberseguridad existentes en Euskadi.

Detallando la metodología implementada se realizó además un mapeo de todos los agentes participantes en el ecosistema, presentando un listado que contemplaba:

1. Todas aquellas organizaciones, creadas o no en Euskadi, que tengan oficina permanente en alguno de los 3 territorios históricos y entre cuyos servicios se extiendan de manera total o parcial al ámbito de la ciberseguridad.
2. Este libro sirve de resumen de la oferta de capacidades de ciberseguridad en Euskadi, que se distribuyen según las taxonomías aplicadas y definidas en el mismo.
3. La taxonomía de ciberseguridad propuesta establece varios niveles, en los que principalmente podemos diferenciar los correspondientes a productos y servicios. Esta clasificación permite conocer en detalle los servicios y productos que se encuentran actualmente en el mercado de la ciberseguridad. Así, el alcance de los productos y servicios permite identificar las principales áreas a las que afectan cada uno de ellos Estos alcances permiten realizar búsquedas y clasificaciones de forma sencilla, dado que además de utilizar categorías, permite buscar en función del área o ámbito en el que se desea aplicar.
4. Para este libro se han identificado diferentes actores del mercado, tanto para la parte de la cadena de suministro que hacen llegar a los usuarios los productos (fabricantes, mayoristas / distribuidores e integradores / consultores), como los que ofrecen servicios.

Se incluyó la ficha de 106 agentes de ciberseguridad con sede en Euskadi.

Y por último, un apartado de conclusiones a modo de resumen ejecutivo.

Segunda edición del libro blanco de la ciberseguridad de Euskadi

El Libro Blanco de la ciberseguridad en Euskadi pretende servir de resumen o instantánea del mercado de la ciberseguridad en Euskadi, siendo el mismo un catálogo vivo que será revisado periódicamente y actualizado según corresponda, ya que se encuentra en constante evolución debido al creciente avance en la digitalización de los servicios y las oportunidades que esto genera.

https://www.basquecybersecurity.eus/archivos/202102/bcsc_libro-blanco_01-2020_15.pdf

En esta segunda edición, además de profundizar en la evolución del sector de la ciberseguridad, haciendo foco en la ciberseguridad industrial, se mapeó cerca de 50 agentes más y se modificó la forma de presentar los datos en forma de ficha alineándolos con la taxonomía propuesta por la asociación público - privada ECSO y basada en el framework del NIST.

2.2. OBJETO

El objeto del presente contrato es la **elaboración de la tercera edición del libro blanco de ciberseguridad en Euskadi**. Para ello, se debe tener en cuenta la documentación referenciada en el punto anterior de antecedentes.

Como referencia, indicar que queremos diferenciar claramente tres aspectos del mismo:

1.Sobre la base de ediciones anteriores, un análisis pormenorizado del sector de ciberseguridad, tanto a nivel mundial como a nivel local de Euskadi. Además de la foto general, es requerimiento que se incluya en la medida de lo posible, toda la información relativa a ciberseguridad industrial específicamente y a la industria vasca de ciberseguridad.

2. Para esta tercera edición, además de identificar a los agentes integrantes del ecosistema, queremos poder clasificarlos en 3 categorías diferentes, en función del nivel de solvencia de las mismas. Planteamos de inicio la posibilidad de que esta forma de clasificación sea listado, acreditado y verificado, pero es labor de la empresa adjudicataria el realizar la propuesta de cuál será el detalle de la clasificación más adecuada atendiendo a la sensibilidad de los agentes y el grado de madurez del sector.

3. Será labor de la empresa adjudicataria, entrevistar y obtener de todos los agentes, la información y evidencias necesarias para ubicar adecuadamente a cada uno de ellos en las categorías seleccionadas y actualizar su ficha.

3. DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR

3.1. CONSIDERACIONES PREVIAS

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 el BCSC, 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 considerarán positivamente en la valoración técnica de la oferta.

El adjudicatario deberá aportar y describir 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.

3.2. ACTIVIDADES OBJETO DEL CONTRATO

El objeto del presente contrato es la elaboración de la tercera edición del libro blanco de ciberseguridad en Euskadi. Para ello, se debe tener en cuenta la documentación referenciada en el punto 2.1.

La taxonomía de agentes de la ciberseguridad partirá de la definida en el Libro Blanco de la Ciberseguridad en Euskadi que describe la oferta en la industria de la ciberseguridad.

3.2.1. CONTEXTUALIZACIÓN DEL ECOSISTEMA

El objetivo de este trabajo es realizar una contextualización del ecosistema vasco de ciberseguridad identificando los factores locales, regionales, estatales, europeos y mundiales que influyen en el mismo. Para ello, al menos, se deberá analizar lo siguiente:

1. Determinar las principales magnitudes del sector de la ciberseguridad: Recopilar los últimos datos disponibles del sector de la ciberseguridad teniendo en cuenta la evolución de los últimos años y las predicciones para los años venideros. Deberán incluirse las referencias de los datos incluidos y se organizarán a nivel internacional, nacional y Euskadi. Se requerirán al menos datos económicos, empleo, cibercrimen y emprendimiento.
2. Recopilación y análisis de los principales hubs de ciberseguridad europeos, mención a las principales magnitudes y especialización de los mismos.
3. En la medida de los posible, análisis de la ciberseguridad industrial, evolución y tendencias, principales retos y toda aquella información relevante sobre la misma que se pueda recopilar a nivel internacional, europeo, español y de nuestro ecosistema.
4. Recopilación de datos del ecosistema de ciberseguridad en Euskadi: El objetivo de este trabajo es realizar una revisión y puesta al día de los datos del sector de ciberseguridad en Euskadi enfocado en los siguientes públicos objetivos:
    a. Clusters y asociaciones, empresas y pymes consumidoras de productos y soluciones de ciberseguridad (lo que se puede entender como la demanda).
    b. Proveedores de productos y soluciones de ciberseguridad (lo que se puede entender como la oferta). Aquí es necesario diferenciar claramente las startups o las empresas de alto potencial de crecimiento.
    c. Administración pública.
    d. Profesionales de ciberseguridad.
    e. Estudiantes de ciberseguridad.
    f. Ciudadanía.
5. Censo de los eventos especializados en ciberseguridad que tienen lugar en el mundo de especial relevancia, indicando el sector y público objetivo al que va dirigido.

3.2.2. DEFINICION DE CRITERIOS DE CATEGORIZACIÓN DE AGENTES

En este momento, en el catálogo de agentes identificados dentro del libro blanco, conviven al mismo nivel empresas que instalan firewalls y se identifican por ello como proveedores de servicios de ciberseguridad y empresas con más de 20 años de trayectoria como fabricantes de productos de ciberseguridad reconocidos a nivel internacional.

El proceso para aparecer en este catálogo consiste únicamente en que nos envíen cumplimentados una serie de datos que les solicitamos. Una vez nos lo envían, no realizamos ningún tipo de verificación sobre la información que nos hacen llegar. Los incluimos en el catálogo y les autorizamos a que usen el sello de “Empresa registrada en el catálogo de ciberseguridad de Euskadi”.

Para esta tercera edición del libro blanco, no queremos solamente listar a los agentes de nuestro ecosistema, **queremos poder establecer una categorización a 3 niveles para poder realmente segmentar la oferta.**

El objetivo de este trabajo es realizar la definición y proponer una metodología para la categorización de los agentes de ciberseguridad en tres niveles dentro de nuestro catálogo: listados, acreditados y verificados.

- Listado: será el nivel más básico en el que al menos se requerirá que las empresas cumplimenten una ficha de agente, proporcionada por el BCSC sobre la que se podrán aplicar mejoras.
- Acreditado: será el nivel medio en el que además de tener que realizar las tareas para ser listados, se solicitará información extra que acredite su respuesta.

- Verificado: será el nivel más alto en el que además de tener que realizar las tareas para ser acreditados, se solicitará una verificación del nivel de madurez de los servicios o productos que proveen.

Es la empresa adjudicataria, **teniendo en cuenta la sensibilidad y grado de madurez del sector y de las propias empresas, quien tiene que determinar el contenido de cada una de las categorías, el grado de exigencia para ubicarse en cada una de ellas y las evidencias a recopilar para garantizar la correcta categorización de las mismas.**

Se tendrá que detallar para cada nivel el proceso a realizar, con una descripción de las tareas llevadas a cabo por las diferentes partes implicadas y los criterios utilizados para cada categorización.

Será necesario realizar una distinción entre proveedores de servicios y proveedores de productos, pudiendo ser diferente la documentación a solicitar.

Los esfuerzos para los agentes tendrán que ser proporcionales al nivel que desee obtenerse. Además, la empresa adjudicataria deberá plantear cómo puede escalar una empresa de un nivel a otro y los incentivos a ofrecer para que puedan evolucionar en la categorización. (A modo de ejemplo y sin que sirva de precedente válido: que sea necesario tener una certificación concreta para estar en una categorización y que pueda ofertarse un programa de ayudas con dicho objetivo).

Se valorará positivamente el basarse en procesos similares reconocidos internacionalmente.

3.2.3. SEGMENTACIÓN DE LOS AGENTES DEL ECOSISTEMA DE LA CIBERSEGURIDAD

Una vez determinadas las categorías de segmentación y teniendo en cuenta todo lo puntualizado en el punto anterior, es labor del adjudicatario de la licitación, la segmentación de los agentes del ecosistema de ciberseguridad dentro de las 3 categorías establecidas.

Esta actividad no sobrepasará el alcance de 200 organizaciones y de ellas, entre 30 y 40 serán startups.

El objetivo de este trabajo es realizar una revisión y puesta al día del sector de ciberseguridad identificando a los agentes de tal modo que se realice la toma de toda la información necesaria de cada organización. La toma de datos se adaptará a la categorización a la que cada empresa quiera aplicar. Esta tarea se podrá realizar de forma presencial, telemática, telefónica y/o email, siendo éstas complementarias.

El adjudicatario es el encargado de recopilar, analizar y validar todas aquellas evidencias que haya determinado que se deben cumplir para ubicar adecuadamente a cada agente en una categoría concreta.

Desde el BCSC podrá realizarse la introducción del adjudicatario a los diferentes agentes, para que no sea una llamada a puerta fría, dando contexto del objetivo, tanto del estudio como de la segmentación.

El entregable de este proceso será las fichas de cada una de las empresas, actualizada si ya estaba lista, o nueva si es de reciente aparición, junto con toda aquella documentación que sea necesaria para garantiza su correcta segmentación.

3.3. PLANIFICACIÓN DE ACTIVIDADES Y METODOLOGÍA

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 (3.2 Actividades objeto del contrato).

En la metodología, la empresa licitadora deberá detallar la forma en la que abordará cada una de las 3 fases definidas para el proyecto: contextualización del ecosistema, criterios de

categorización de agentes y segmentación de los mismos. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

Dicha propuesta deberá estar basada en su experiencia e incluirá una descripción que detalle cada tarea y la defina con el mayor grado de profundidad posible.

Entendemos que la fase 1 y la fase 2 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 cumpla el hito de entrega final en los tiempos especificados.

La empresa licitadora deberá presentar una propuesta inicial de las tareas, hitos y entregables.

3.4. EQUIPO DE TRABAJO

3.4.1. COMPOSICIÓN

El equipo estará formado por el número de profesionales 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. De igual forma, el equipo podrá balancearse de tal forma que no todas las personas tengan que tener una dedicación total y exclusiva al proyecto durante toda la duración del mismo.

3.4.2. PERFILES ADSCRITOS AL PROYECTO

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:

- Conocimiento demostrable de los entornos de ciberseguridad vasco y global.
- Haber participado en proyectos de similar naturaleza al objeto del presente pliego.

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 Vasco, SPRI, y/o sociedades participadas por los mismos, tanto durante la vigencia del contrato como al término de este.

3.5. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto en SPRI, 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, BCSC indicará al comienzo del proyecto, la persona designada como Director de Proyecto en SPRI 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, el Director 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 que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio del Director 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.

3.6. 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 el Director 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 el Director 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 el Director de Proyecto. Toda la documentación generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva de SPRI sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de SPRI, que la concederá, en su caso y con expresión del fin, previa petición formal del adjudicatario.

En este sentido, el adjudicatario deberá informar al Director 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 el Director 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.

3.7. ENTREGABLES

Al finalizar los trabajos se deberá de presentar los siguientes entregables validados por el adjudicatario:

1. Criterio de clasificación de empresas: Documento para uso interno del BCSC en el que se justifiquen adecuadamente los criterios de clasificación en las 3 categorías, junto con una serie de recomendaciones para incentivar a las empresas a corto, medio o largo plazo para cambiar de categoría.
2. Tercera edición del Libro blanco de ciberseguridad en Euskadi, con el listado actualizado de agentes, pero sin la segmentación de los mismos, en formato editable.
3. Tercera edición de Libro blanco de ciberseguridad en Euskadi completo, incluyendo la segmentación de los agentes, en formato editable.
4. Fichas individuales y evidencias de cada agente registrado en el catálogo.
5. Fichero agregado de agentes registrados en el catálogo.

6. Los editables de todos los elementos incluidos en el estudio.

La fecha límite para la entrega completa de todos los entregables será de máximo 6 meses desde el inicio del proyecto, valorándose positivamente la entrega en un plazo inferior. Se establece una entrega parcial, que incluye los entregables 1 y 2 de este listado (Criterio de clasificación de empresas y tercera edición del libro blanco con el listado de agentes actualizado pero sin segmentación de los mismos), que deberán realizarse con anterioridad al 31 de diciembre de 2021.