0 ANTECEDENTES

BiscayTIK es un proyecto promovido por la Diputación Foral de Bizkaia, con un marcado carácter innovador y pionero a nivel internacional, que tiene como objetivos acercar la Administración a la ciudadanía a través de un nuevo canal de comunicación, vía Internet, facilitándoles la interactuación entre ambos, homogeneizar las herramientas informáticas de los Ayuntamientos de Bizkaia para la mejora de su gestión interna y de su relación con los ciudadanos y las ciudadanas y convertir Bizkaia en referente internacional para la aplicación en las tecnologías de la información y el conocimiento en la Administración Municipal.

Para cumplir este objetivo el proyecto cuenta con tres ejes,

- Servicio de correo electrónico para la ciudadanía.
- Programas informáticos para los municipios y portal web de tramitación Ciudadana.
- Creación de un Centro Tecnológico de referencia internacional.

La seguridad de la información, durante los últimos años, ha cobrado protagonismo por la dependencia universal de sistemas seguros, fiables y resilientes, alcanzando tanto al sector público como al privado, desarrollándose en un marco normativo desconocido hasta el momento. Tanto la normativa europea, reflejada en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, así como la normativa derivada del ENS, afrontan una visión conjunta, europeísta, incrementando el nivel de ciberseguridad de los sistemas de información. La evolución de las tecnologías de la información, especialmente con el desarrollo de Internet asociado a su obligada presencia de todos los actores del Sector Público, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Esta situación ha servido para tomar consciencia de la importancia que puede suponer para una organización los incidentes que, al afectar a las redes y sistemas de información, alteren sus actividades cotidianas, representando una grave amenaza, pues tanto si los mismos son fortuitos como si provienen de acciones deliberadas pueden menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia integridad de las instituciones.

Considerando el despliegue horizontal e interconectado de las tecnologías de la información en todo el Sector Público, que supone una mayor extensión de sus amenazas y riesgos, permite vislumbrar que para adoptar medidas eficaces que contrarresten esos riegos debe realizarse una planificación que observe el todo, evitando acciones aisladas. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos afectados.

Por tanto, desde Fundación BiscayTIK Fundazioa, se considera oportuno establecer un proyecto que, con una perspectiva integral, permita realizar un estudio para mejorar la protección frente a las amenazas que afecten a los sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia para las entidades locales (EELL) del Territorio Histórico de Bizkaia (THB).

1 OBJETO

El objeto del presente concurso es la contratación del servicio de consultoría para la definición del plan de acción de la implantación de un centro de operaciones de seguridad para las Entidades Locales del Territorio Histórico de Bizkaia adheridas al proyecto BiscayTIK.

2 ESPECIFICACIONES TÉCNICAS

La adjudicataria deberá tener la capacidad de prestar una gestión de proyectos y un asesoramiento consultivo integral a la entidad contratante, poniendo inmediatamente a disposición del contrato especialistas en todas las materias que comprenden el servicio de consultoría para la definición del plan de acción de la implantación de un centro de operaciones de seguridad para las Entidades Locales del Territorio Histórico de Bizkaia adheridas al proyecto BiscayTIK.

La prestación del servicio será ejecutada por la adjudicataria con calidad, rigor y eficacia y con absoluto cumplimiento de todas las disposiciones legales, reglamentarias, normas y especificaciones en vigor que, de forma directa e indirecta, regulen el mismo.

Se deberá designar una persona responsable de supervisar en todo momento la buena marcha de las actividades objeto del contrato.

El adjudicatario ejercerá el control y supervisión del personal que preste el servicio, sustituyéndolo en caso de enfermedad, vacaciones y ausencias con otro personal cualificado.

El servicio podrá ser prestado por diferentes canales: correo, telemático, telefónico o presencial.

En todo caso, los trabajos se realizarán a petición de Fundación BiscayTIK Fundazioa sin perjuicio de que Fundación BiscayTIK Fundazioa pueda contratar con otras empresas adjudicatarias las materias objeto de este pliego.

2.1 Descripción general de la prestación

La percepción de las amenazas utilizando medios electrónicos se han convertido en una realidad plausible, universal y creíble, formando parte del conocimiento general, resultando un potente instrumento de agresión contra las entidades públicas y las personas en sus relaciones con las mismas, de manera que la ciberseguridad tiene que convertirse en un ámbito prioritario de actuación de toda entidad pública. Por ello, se requiere de mantener unas garantías que ofrezcan seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas, generando una estrategia para alcanzar el adecuado nivel de ciberseguridad y resiliencia, mediante la implantación de unos sistemas de Información y Telecomunicaciones que sean coherentes con esos objetivos.

Desde los orígenes de lo que se ha llamado el ámbito de la administración electrónica, el esquema nacional de seguridad ha dispuesto de un especial señalamiento en la normativa reguladora. El artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, establecía la creación del Esquema Nacional de Seguridad, cuyo objeto sería el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permitiese la adecuada protección de la información. Este concepto tomó cuerpo con la aprobación del Real Decreto 3/2010, de 8 de enero, por el que se reguló el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, comenzando su andadura en un período en el que su obligatoriedad se encontraba en entredicho, sobre todo en el ámbito local,

considerando el amplio margen de implantación descrito en la Disposición Transitoria Tercera de dicha norma. Con la derogación de la Ley 11/2007 por el bloque de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la obligatoriedad se estableció uniformemente, requiriendo de una urgente adaptación mediante la aprobación del Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010 para conseguir que la ciudadanía siguiese confiando en que los servicios públicos disponibles por el medio electrónico se prestasen en unas condiciones de seguridad equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de la Administración, precisando, profundizando y contribuyendo al mejor cumplimiento de los mandatos normativos.

Estos servicios de seguridad de prevención, protección, monitorización, detección y respuesta, en el ciberespacio se integrarán y ofrecerán desde la oficina centralizada de ciberseguridad o centro de operaciones de seguridad y permitirán a una entidad local aumentar su capacidad de vigilancia y detección de amenazas en el empleo diario de los sistemas de información y comunicaciones y mejorar su capacidad de respuesta ante cualquier ataque.

En consecuencia y por lo especificado anteriormente, desde la Fundación BiscayTIK se considera necesario proveer a los EELL del THB de un servicio de seguridad que ayude a cumplir con los requisitos establecidos en el ENS e implemente medidas reforzadas de ciberseguridad, tanto técnicas como organizativas, a través de la implantación de una oficina centralizada que dé respuesta a estas necesidades, y es por esto por lo que se considera necesaria la realización de una consultoría para el diseño de dicho centro y la definición del plan de acción detallado para la posterior implantación de dicha oficina.

En definitiva, el resultado de la consultoría proporcionará a BiscayTIK de todas las herramientas técnicas y organizativas necesarias (planes, procesos, modelos, costes, …) para poder implantar un centro de operaciones de ciberseguridad para el cumplimiento de las medidas mínimas del ENS para las entidades locales del Territorio Histórico de Bizkaia.

2.2 Descripción tareas alcance del servicio

A continuación, se detallan las principales actividades relacionadas con el servicio, que, sin ánimo de ser exhaustivas y completas, pretenden describir el marco de trabajo exigible en cuanto a la presente licitación.

Para la consecución del objetivo final y con el propósito de alcanzar las metas descritas en este informe de especificaciones técnicas, se deberá realizar una propuesta técnica que tenga en cuenta todas las fases de la consultoría indicándose tareas, responsables y entregables desde el inicio hasta la obtención del plan director que defina los pasos detallados a dar para la implantación de la oficina de ciberseguridad. De esta manera, se deberán incorporar al menos las siguientes:

2.2.1 Diagnóstico inicial de las entidades locales en materia de ciberseguridad (AS IS)

En esta fase se deberá determinar el estado actual de la gestión de la seguridad y privacidad de la información en todas las entidades locales de Bizkaia, así se identificará el nivel de madurez y las diferentes tipologías de entes que existen en Bizkaia con respecto al grado de cumplimiento de los requisitos marcados en el ENS.

De esta manera se obtendrá una foto inicial que servirá de entrada para la siguiente fase y que será clave a la hora de identificar el GAP entre la situación real actual y la situación objetivo deseada. Además, esta información será de utilidad para la identificación de los servicios y medidas a implementar, la conveniencia o no de agrupación de estos para crear un porfolio de servicios agrupado, los niveles de seguridad requeridos según el

marco normativo, la homogeneidad y/o heterogeneidad entre las entidades locales que permita su agrupación o no y la creación de tipologías de entidades locales a los que ofrecer cada uno de los servicios.

Así mismo se deberán identificar posibles problemas, incompatibilidades, dependencias, etc. que pudiera condicionar el modelo futuro, teniendo siempre en cuenta que el objetivo final es que el alcance del servicio abarque a la totalidad de las entidades locales del Territorio Histórico de Bizkaia por lo que habrá que preparar un plan de acción para que dichos posibles condicionantes no dejasen fuera del servicio a ninguna entidad local.

2.2.2 Definición del modelo objetivo (TO BE) y plan de acción

El objetivo de esta fase es definir y diseñar punto por punto el escenario objetivo y las funciones detalladas del centro de operaciones de seguridad de BiscayTIK y establecer la hoja de ruta para partiendo del escenario actual llegar al modelo objetivo definitivo.

En esta fase se definirán detalladamente todos los servicios que conformen el catálogo que se proponen proveer desde la oficina, y cuáles son las potenciales entidades receptoras, incluyéndose de esta manera una matriz de servicios, entidades y necesidades ad-hoc para cada una de ellas basado en el informe de diagnóstico de la situación inicial. Se realizará, así mismo, la definición de todos y cada uno de los procedimientos y planes enfocados a la gestión, seguimiento y mejora continua además de la definición de los reportes tanto externos como internos propuestos.

El plan de acción de la implantación de la oficina de operaciones de ciberseguridad deberá detallar las acciones concretas a realizar para cada iniciativa que comprenda el plan, desarrollar los planes para la implantación de cada una de las acciones identificadas, planificación temporal de estas, recursos necesarios para cada una, la dedicación de la Fundación y/u otras dependencias externas, así como una estimación económica de la implantación y ejecución del plan propuesto. Además, se deberá plantear una estrategia de implantación de este en base a los servicios identificados y las entidades locales receptoras de los mismos.

Por último, se deberá indicar el modelo de gestión y gobernanza del servicio futuro, describiéndose el modelo organizativo, el modelo operativo y el modelo de gestión del servicio.

Las ofertas, al menos, deberán especificar claramente el entendimiento del alcance, así como el enfoque completo propuesto para obtener todos los objetivos especificados en el presente informe de especificaciones técnicas, identificándose y describiéndose la metodología a utilizar en cada fase identificada o fases propuestas por el licitador, las tareas concretas que se compromete a realizar, la organización y equipo de trabajo y el plan de proyecto propuesto representado en un diagrama de Gantt y conteniendo al menos las actividades, hitos, plazos, entregables y equipo asignado a cada una de las fases propuestas.

Por las necesidades del servicio y teniendo en cuenta la fase de diagnóstico inicial de las entidades locales en materia de ciberseguridad (AS IS) y la necesidad de relación con diferentes entidades locales, el servicio deberá ser prestado en bilingüe (euskera y castellano), tanto a nivel conversacional como a nivel documental.

2.2.3 Condiciones especiales de compatibilidad

De la definición del modelo objetivo (TO BE) y plan de acción no podrán resultar unas soluciones tan concretas y delimitadas que únicamente se ajusten a las características técnicas del adjudicatario, de cara a un eventual contrato para la implantación de dicho modelo y plan de acción. El resultado de la definición del modelo objetivo (TO BE) y plan de acción deberá concretarse en la introducción de características genéricas, exigencias generales o fórmulas abstractas que aseguren una mejor satisfacción de los intereses públicos, sin que, en ningún caso,

puedan comportar ventajas para el adjudicatario respecto de la adjudicación de un eventual contrato para la implantación de aquel modelo.

El adjudicatario de este contrato podrá participar en la nueva y eventual licitación para la implantación del modelo objetivo y plan de acción. En dicha licitación, se adoptarán las siguientes medidas:

- Se pondrá a disposición de las empresas licitadoras interesadas la documentación de diagnóstico y la definición del modelo objetivo y plan de acción entregados por la adjudicataria de este contrato, salvaguardando la información confidencial que corresponda, a fin de que pueda servir de información para la preparación de la oferta por las demás licitadoras.
- Se identificará a la adjudicataria autora de dicha documentación.
- Se establecerá un plazo adecuado para la presentación de ofertas.

3 CONTROL Y SEGUIMIENTO

El objetivo de las tareas que la empresa licitadora tiene que proponer en este apartado, están destinadas a poder disponer en todo momento de una visión del estado del servicio prestado, con el fin de poder identificar posibles desviaciones y sus acciones correctoras.

La base para poder realizar estas labores son los informes de seguimiento, que serán revisados en las reuniones y comités correspondientes.

La empresa licitadora tendrá que describir en su propuesta técnica el modelo de control de seguimiento propuesto que será aplicado durante la prestación del servicio con el máximo detalle posible.

Fundación BiscayTIK Fundazioa nombrará una persona que será la encargada de supervisar su desarrollo y aprobar su resultado final, transmitiendo a la empresa adjudicataria cuantas instrucciones considere necesarias.

La empresa adjudicataria establecerá una persona responsable única con Fundación BiscayTIK Fundazioa, que recibirá instrucciones generales por parte de Fundación BiscayTIK Fundazioa interviniendo como interlocutor de esta responsabilidad. Se encargará:

- Planificación, seguimiento y control de los trabajos a realizar y de verificar su nivel de calidad.
- Recepción de peticiones por parte de la Fundación BiscayTIK Fundazioa, peticiones que deberá valorar y planificar en acuerdo con Fundación BiscayTIK Fundazioa.
- Realización de las actas de reunión mantenidas con Fundación BiscayTIK Fundazioa donde se establezcan los acuerdos alcanzados. Se establecerá inicialmente una periodicidad semanal de las reuniones, cuyo objetivo principal será realizar el seguimiento de las tareas en curso, identificar desviaciones, así como puntos críticos o paralizantes del avance de las mismas.

La persona coordinadora del equipo de trabajo deberá poder presentarse en Fundación BiscayTIK Fundazioa, en menos de dos horas si Fundación BiscayTIK Fundazioa así lo requiriese.

A la finalización de los trabajos, la empresa adjudicataria facturará los trabajos en base a la valoración aceptada. Fundación BiscayTIK Fundazioa revisará los trabajos efectivamente entregados, y dará su VB° a los mismos.

La Fundación BiscayTIK Fundazioa se reserva el control de calidad de los trabajos realizados, pudiendo rechazar aquellos que no cumplan las condiciones mínimas, de acuerdo con sus propios criterios; todo ello, con independencia de las penalizaciones que Fundación BiscayTIK Fundazioa pueda imponer como consecuencia de

los retrasos o bajas calidades de los servicios contratados, siendo así mismo causa justificada de resolución contractual.

4 CONDICIONES PARTICULARES

Las empresas licitadoras, en la elaboración y presentación de sus respectivas propuestas deberán hacer un uso no sexista del lenguaje. Asimismo, la empresa adjudicataria, a lo largo de la vigencia del contrato, deberá hacer un uso no sexista del lenguaje en cualquier documento definitivo escrito o digital, así como, deberá desagregar los datos por sexo en cualquier estadística referida a personas que se genere, todo ello al amparo del artículo 2.3 de la Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres en el que se señalan los principios generales que deberán respetarse.

4.1 Equipo de trabajo y requisitos

La empresa adjudicataria deberá aportar los recursos humanos y materiales necesarios para la correcta realización de los servicios que se le encarguen.

La empresa adjudicataria tendrá plena movilidad geográfica y deberá prestar los servicios allá donde lo requiera BiscayTIK, debiendo desplazar todo o parte de su equipo, según resulte preciso, sin cargo adicional alguno. Igualmente, la adjudicataria se compromete a mantener y atender las reuniones que BiscayTIK concierte con otras empresas o instituciones.

Cualquier cambio en la composición del equipo durante la vigencia del contrato no podrá variar la acreditación aportada en la memoria descriptiva, deberá notificarse previamente a Fundación BiscayTIK Fundazioa y contar con la autorización expresa de Fundación BiscayTIK Fundazioa

La empresa adjudicataria se encargará de mantener permanentemente formado a su personal en aquellas tecnologías/funcionalidades que Fundación BiscayTIK Fundazioa vaya demandando. El costo de esta formación, así como la dedicación que el personal de la empresa adjudicataria emplee en esta formación correrán por cuenta de ésta sin que, de ningún modo, pueda imputarse a Fundación BiscayTIK Fundazioa en costo y/o tiempo dedicado al contrato.

Los equipos, licencias, comunicaciones y desplazamientos necesarios del personal de la empresa adjudicataria serán a cargo de ésta.

La adjudicataria ejercerá el control y supervisión del personal que preste el servicio, sustituyéndolo en caso de enfermedad, vacaciones y ausencias con otro personal cualificado.

Dentro del equipo de trabajo habrá roles según las siguientes tipologías:

- Jefatura de proyecto: realizará las labores de coordinación con Fundación BiscayTIK Fundazioa. Esta persona será responsable única con Fundación BiscayTIK, no teniendo porque tener dedicación exclusiva, y se encargará de la planificación, seguimiento y control de los trabajos a realizar y de verificar su nivel de calidad. Dicha persona será la que reciba instrucciones generales por parte de Fundación BiscayTIK interviniendo como interlocutor de esta responsabilidad. Adicionalmente, será el perfil vertebrador de los trabajos objeto de este contrato.
- Consultoría experta en seguridad: serán los responsables de la correcta ejecución del contrato y del desarrollo de los trabajos en él incluidos, garantizando la calidad de los entregables previstos durante toda la ejecución del contrato.

Para la realización del servicio la empresa licitadora deberá ofertar un equipo de trabajo con la solvencia técnica necesaria para la realización de los trabajos. Se considera necesario al menos un equipo de trabajo formado por:

- Al menos una (1) persona con perfil de jefatura de proyecto con al menos cinco (5) años de experiencia contrastada en la gestión de proyectos en el ámbito de la presente licitación y experiencia en consultorías de seguridad cuyo marco de referencia haya sido el Esquema Nacional de Seguridad u otro estándar de referencia. Se requiere, al menos estar en posesión del título de licenciatura o ingeniería en informática o similar y las siguientes certificaciones profesionales:
    - Obligatoriamente alguna de las siguientes:
        - PMP (Project Management Professional) o PRINCE2 (Projects In Controlled Environments) o ITIL (Service Management Foundation Certification) o similar.
    - Serán valorables:
        - CISA (Certified Information Systems Auditor).
        - CRISC (Certified in Risk and Information Systems Control).
        - CISSP – ISSMP (Information Systems Security Management Professional).
        - CISSP – ISSAP (Information Systems Security Arquitecture Professional).
        - Lead Auditor ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar).
        - Lead Implementer ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar).
        - Otras similares a las anteriores.
- Al menos dos (2) personas con perfil consultoría experta en seguridad con al menos tres (3) años de experiencia profesional demostrable en consultorías de seguridad del ámbito del presente proyecto. Se requiere, al menos estar en posesión del título de licenciatura o ingeniería en informática o similar y las siguientes certificaciones profesionales para cada uno de los consultores propuestos:
    - Obligatoriamente al menos una de las siguientes:
        - CISA (Certified Information Systems Auditor)
        - CRISC (Certified in Risk and Information Systems Control).
        - CISSP (Certified Information Systems Security Professional).
        - CISM (Certified Information Security Manager).
        - CISSP – ISSAP (Information Systems Security Arquitecture Professional).
        - Lead Auditor ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar).
        - Lead Implementer ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar).
        - Otras similares a las anteriores.

Una persona del equipo de trabajo deberá hablar y escribir en castellano y euskera indistintamente como lengua nativa o ser capaz de comunicase en castellano y euskera de forma fluida, pudiendo ser el interlocutor en cualquier ámbito del alcance del proyecto.

El equipo propuesto por la empresa licitadora en la oferta podrá estar formado por un número de personas superior al que se solicita como solvencia técnica mínima. Se deberán cumplimentar las tablas de detalle-1 y detalle-2 del Anexo I de este informe para todas las personas que formen parte del equipo de proyecto. Este

punto será valorado dando mayor puntuación a la empresa licitadora que proponga un equipo mejor dimensionado.

Entre todos los perfiles que formen parte del equipo de trabajo se deberá cubrir al menos las certificaciones de CISA (Certified Information Systems Auditor) y Lead Auditor ISO 27001.

El equipo propuesto por el proveedor deberá cumplir los requisitos exigidos en el apartado 16.b de la carátula.

4.2 Entregables del Proyecto

La empresa licitadora deberá indicar claramente cuáles son los entregables resultado del proyecto que comprende su propuesta, siendo obligatorio la elaboración del informe de diagnóstico de la situación inicial, el plan final detallado para la implantación de una centro de operaciones de ciberseguridad para las EELL del THB así como un informe que responda al diseño de dicho centro.

En las ofertas se deberá aportar una propuesta de los índices de todos los documentos que se compromete a realizar la empresa licitadora dentro del alcance de la consultoría. Tanto los entregables propuestos como el nivel detalle de los índices será valorado en la oferta técnica. Este punto será valorado dando mayor puntuación a la empresa licitadora que proponga mejor calidad y detalle en dichos entregables.

4.3 Planificación e hitos de entrega

El licitador deberá realizar los trabajos objeto de este contrato en el plazo máximo indicado en el apartado 5 de la carátula. El licitador deberá indicar en su propuesta una planificación detallada, representada en un diagrama de Gantt, con fases, plazos, recursos, cargas y los distintos hitos de entrega de los entregables objeto del proyecto.

Se valorará la mejora en la planificación y su nivel de detalle.

4.4 Control de los trabajos

La Fundación BiscayTIK Fundazioa se reserva el control de calidad de los trabajos realizados, pudiendo rechazar aquellos que no cumplan las condiciones mínimas, de acuerdo con sus propios criterios; todo ello, con independencia de las penalizaciones que BiscayTIK pueda imponer como consecuencia de los retrasos o bajas calidades de los servicios contratados, siendo así mismo causa justificada de resolución contractual.

La empresa adjudicataria propondrá soluciones mecanizadas para la gestión y seguimiento del servicio.

4.5 Propiedad intelectual

La adjudicataria cederá a favor de la Fundación BiscayTIK Fundazioa todos sus derechos de autor y de propiedad intelectual, en general, correspondientes a los trabajos, creaciones y documentos preparados en virtud del presente contrato. La cesión de los derechos de propiedad intelectual no tendrá límite temporal alguno y se entenderá incluida en los honorarios a cobrar por la adjudicataria. A tales efectos la Fundación BiscayTIK Fundazioa estará legitimada para modificar, transformar, reproducir, distribuir, publicar, exponer, utilizar y explotar en general la obra del adjudicatario.

La adjudicataria se obliga a no utilizar, directa o indirectamente, todo o parte del Estudio para cualquier otro encargo similar que se pudiera desarrollar en cualquier lugar del mundo.

La empresa adjudicataria debe facilitar a Fundación BiscayTIK Fundazioa todas las fuentes de todos los archivos, así como de los recursos tecnológicos empleados.

4.6 Garantía

Se exigirá una garantía mínima de 3 meses para los trabajos realizados.

4.7 Perspectiva de género

Las empresas licitadoras, en la elaboración y presentación de sus respectivas propuestas deberán hacer un uso no sexista del lenguaje. Asimismo, la empresa adjudicataria, a lo largo de la vigencia del contrato, deberá hacer un uso no sexista del lenguaje en cualquier documento definitivo escrito o digital, así como, deberá desagregar los datos por sexo en cualquier estadística referida a personas que se genere, todo ello al amparo del artículo 2.3 de la Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres en el que se señalan los principios generales que deberán respetarse.

La empresa adjudicataria presentará en la justificación final de la realización de la prestación objeto del contrato, en su caso, una memoria sobre el impacto de género de la contratación, con los indicadores y datos desagregados por sexo de las personas usuarias o beneficiarias, o del personal prestador del servicio, que posibiliten evaluar la eficacia de las medidas de igualdad aplicadas.

Firmado: Alaitz Etxeandia Arteaga

Directora General Fundación BiscayTIK Fundazioa

ANEXO I – SOLVENCIA EQUIPO HUMANO

Requisitos técnicos mínimos	Valor Propuesto	Valor Exigido
Persona **jefatura de proyecto** con al menos cinco (5) años de experiencia contrastada en la gestión de proyectos en el ámbito del presente proyecto y experiencia en consultorías de seguridad cuyo marco de referencia haya sido el Esquema Nacional de Seguridad u otro estándar de referencia. Se requiere, al menos estar en posesión del título de licenciatura o ingeniería en informática o similar y las siguientes certificaciones profesionales: • Obligatoriamente alguna de las siguientes: o PMP (Project Management Professional) o PRINCE2 (Projects In Controlled Environments) o ITIL (Service Management Foundation Certification) o similar. • Serán valorables: o CISA (Certified Information Systems Auditor). o CRISC (Certified in Risk and Information Systems Control). o CISSP – ISSMP (Information Systems Security Management Professional). o CISSP – ISSAP (Information Systems Security Arquitecture Professional). o Lead Auditor ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar). o Lead Implementer ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar). o Otras similares a las anteriores.	(en años) Licenciatura, Ingeniería en Informática o similar (SÍ / NO) Experiencia Consultorías marco ENS u otro (SÍ / NO) (indicar al menos 2 en tabla detalle-1) Cumple (SÍ / NO) (Cumplimentar en la tabla detalle-2) Cumple (SÍ / NO) (Cumplimentar en la tabla detalle-2)	>=5 años SÍ SÍ SÍ al menos uno N/A
El licitador deberá disponer en el equipo de al menos dos (2) personas con **perfil consultoría experta en seguridad** con al menos tres (3) años de experiencia profesional demostrable en consultorías de seguridad del ámbito del presente proyecto. Se requiere, al menos estar en posesión del título de licenciatura o ingeniería en informática o similar y las siguientes certificaciones profesionales para cada uno de los consultores propuestos: • Obligatoriamente al menos un de las siguientes: o CISA (Certified Information Systems Auditor) o CRISC (Certified in Risk and Information Systems Control). o CISSP (Certified Information Systems Security Professional). o CISM (Certified Information Security Manager). o CISSP – ISSAP (Information Systems Security Arquitecture Professional).	Persona Consultora 1 (en años) Licenciatura, Ingeniería en Informática o similar (SÍ / NO) Experiencia en Consultorías de seguridad (SÍ / NO) (Indicar al menos 2 en la tabla detalle-1) Certificaciones (Indicar al menos 1 en la tabla detalle-2)	>=3 años SÍ SÍ

○ Lead Auditor ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar). ○ Lead Implementer ISO 27001 (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI o similar). ○ Otras similares a las anteriores.	Persona Consultora 2 (en años) Licenciatura, Ingeniería en Informática o similar (SÍ / NO) Experiencia en Consultorías de seguridad (SÍ / NO) (Indicar al menos 2 en la tabla detalle-1) Certificaciones (Indicar al menos 1 en la tabla detalle-2)	>=3 años SÍ SÍ

Tabla de detalle-1

Perfil	Descripción proyecto	Cliente	Fecha inicio	Fecha fin	Importe (€ sin IVA)
Jefatura Proyecto			mes/año	mes/año	
			mes/año	mes/año	
	...	...	...	...	...
Consultoría 1			mes/año	mes/año	
			mes/año	mes/año	
	...	...	...	...	...
Consultoría 2			mes/año	mes/año	
			mes/año	mes/año	
	...	...	...	...	...

Indicar al menos 2 (dos) proyectos para cada perfil para los perfiles que forman parte de la solvencia técnica.

Cumplimentar otra tabla separada como esta para el resto de los perfiles que forman parte del equipo de proyecto propuesto aun cuando no formen parte de la solvencia técnica.

Tabla de detalle 2

Perfil	Bilingüe euskera-castellano (SÍ / NO)	Titulación académica	Certificación Gestión Proyectos	Certificación Seguridad
Jefatura Proyecto				
Consultoría 1				
Consultoría 2				

Indicar todas las certificaciones para cada perfil. Las certificaciones profesionales deberán estar vigentes en el momento de la adjudicación y mantenerse a lo largo de toda la ejecución del contrato.

Al menos un perfil deberá ser bilingüe euskera-castellano.

Entre todos los perfiles que formen parte del equipo de trabajo se deberá cubrir al menos las certificaciones de CISA (Certified Information Systems Auditor) y Lead Auditor ISO 27001.

Cumplimentar otra tabla separada como esta para el resto de los perfiles que forman parte del equipo de proyecto propuesto aun cuando no formen parte de la solvencia técnica.

El incumplimiento de estos requerimientos para el equipo propuesto será causa de exclusión. La NO inclusión explicita de esta información para cualquiera de los perfiles, será interpretada como no cumplimiento.