Expediente: "SERVICIO DE OFICINA TÉCNICA DE SEGURIDAD PARA LA AGENCIA VASCA DE CIBERSEGURIDAD"

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Índice

1 INTRODUCCIÓN 3
2 OBJETO DEL CONTRATO 5
3 TAREAS A REALIZAR 7
3.1 LOTE 1 – Cumplimiento Normativo 7
3.2 LOTE 2 – Gestión de Riesgos 8
3.3 LOTE 3 – Gobernanza de la ciberseguridad 9
4 DEFINICIÓN DEL SERVICIO 11
4.1 Fases del servicio 11
4.1.1 Periodo de transición 11
4.1.2 Prestación regular del servicio 11
4.1.3 Devolución 11
4.2 Entregables 11
4.3 Modelo de prestación del servicio 13
4.4 Equipo de trabajo 13
Responsable del servicio 14
Consultores Senior 14
Especialistas 14
4.5 Dimensionamiento y dedicación 14
LOTE 1 – Cumplimiento Normativo 15
LOTE 2 – Gestión de Riesgos 15
LOTE 3 – Gobernanza de la ciberseguridad 15
5 EJECUCIÓN DEL CONTRATO 16
5.1 Supervisión del contrato 16
5.2 Asignación del Personal 16
5.2.1 Constitución inicial del equipo de trabajo 17
5.2.2 Modificaciones en la composición del equipo de trabajo 17
5.3 Registro y Control 18
6 SEGURIDAD 19
6.1 Secreto y Confidencialidad 19
6.2 Propiedad intelectual 19

1 INTRODUCCIÓN

La Agencia Vasca de Ciberseguridad (Cyberzaintza), en adelante la Agencia, es un ente público de derecho privado del Sector Público de la Comunidad Autónoma Vasca. La Agencia se adscribe al departamento del Gobierno Vasco competente en materia de seguridad, a través de la persona titular de la Viceconsejería de Seguridad.

La Agencia tiene por objeto promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de su competencia, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración Pública, de su ciudadanía y de su tejido empresarial.

La LEY 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad en su Artículo 2 establece que las funciones que corresponden a la Agencia para el cumplimiento de su objeto son las siguientes:

- Promover una estrategia de ciberseguridad para el conjunto de las administraciones públicas de la Comunidad Autónoma Vasca, y potenciar y coordinar el alineamiento en la ciberseguridad en dicho conjunto.
- Impulsar un marco de estándares, directrices y normas técnicas de seguridad recomendables para el sector público vasco.
- Informar, con carácter preceptivo, en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Comunidad Autónoma Vasca en materia de ciberseguridad.
- Realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad desplegadas en el ámbito del sector público vasco.
- Prevenir y detectar incidentes de ciberseguridad en la Comunidad Autónoma Vasca y responder a ellos, estableciendo criterios y promoviendo el despliegue de las medidas de protección pertinentes ante las ciberamenazas y los riesgos inherentes sobre las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan, todo ello con respeto del marco competencial aplicable.
- Recoger los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en la Comunidad Autónoma Vasca en relación con el estado de la seguridad de la información, prestando especial atención a los sistemas considerados como críticos para el funcionamiento de los servicios públicos o la seguridad de las personas, con vistas a informar al Gobierno Vasco, así como a las administraciones públicas del territorio que intervengan en la prestación de dichos servicios críticos y esenciales, y proponer las medidas adecuadas llevando a cabo la gestión de riesgos en materia de ciberseguridad.
- Ejercer las funciones del equipo de respuesta a emergencias (CERT) dentro de las competencias de la Comunidad Autónoma Vasca. Dado que se trata de un fenómeno transfronterizo, es necesario colaborar con las administraciones y agencias de otros territorios con el objetivo de minimizar los daños y el tiempo de recuperación en caso de ciberataque.
- Coordinar los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y los equipos de respuesta a emergencias o las entidades equivalentes que actúen en su ámbito de actuación y de acuerdo a la legislación vigente, estableciendo modelos de colaboración con otros CSIRT estatales e internacionales. Asimismo, la Agencia ejercerá funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad en el ámbito del sector público vasco.
- Trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la

dependencia de productos y servicios de ciberseguridad de fuera de la Unión Europea y reforzar las cadenas de suministro de dentro de la Unión Europea.

- Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información y servicios de tecnologías de la información.
- Garantizar un nivel adecuado de ciberseguridad en el uso de medios electrónicos.
- Organizar actividades de difusión, promoción, formación y concienciación en materia de ciberseguridad.
- Organizar actividades para promocionar el talento en la ciberseguridad, y participar en actividades de ciberseguridad, dando a conocer referentes, haciendo especial hincapié en las mujeres profesionales de la ciberseguridad.
- Proponer medidas técnicas de ciberseguridad en la utilización de los recursos informáticos y de las comunicaciones existentes, y proponer la formación en estas medidas del personal de la Administración de la Comunidad Autónoma Vasca y del propio personal de la Agencia.
- Actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas y, en particular, en las tareas de lucha contra las conductas ilícitas, incluidas la intervención directa y la obtención de pruebas electrónicas.
- Coordinar al sector público vasco en la elaboración de sus respectivos planes de ciberseguridad, así como en la consecución de los objetivos establecidos en los mismos.
- Poner sus servicios materiales y técnicos de ciberseguridad a disposición del sector público vasco.
- Impulsar la coordinación del sector público vasco en todo lo que se considere necesario para la consecución de los objetivos especificados en los planes de ciberseguridad, estableciendo para ello las líneas de colaboración que se entiendan necesarias.
- Ostentar la representación oficial del sector público vasco ante organismos internacionales, estatales y regionales en materia de ciberseguridad.
- Apoyar e impulsar la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial y en los sectores esenciales de la Comunidad Autónoma Vasca, como son el sector sanitario, el sector de emergencias y seguridad, el sector de servicios sociales y de intervención social, el sector educativo, el sector del transporte y el sector de la energía y las telecomunicaciones, o cualquier otro sector que pudiera considerarse sensible.
- Cualesquiera otras competencias que le sean conferidas por la legislación vigente o le sean expresamente delegadas o atribuidas.

La Agencia Vasca de Ciberseguridad necesita contratar una Oficina Técnica de Seguridad que pueda proporcionar servicios especializados en el ámbito del cumplimiento normativo, la gestión de riesgos y la gobernanza de la ciberseguridad, con el fin de apoyar la implantación de una estrategia común y de un modelo de gobernanza que alinee las capacidades de ciberseguridad existentes.

El contrato se divide en tres lotes: cumplimiento normativo, gestión de riesgos y gobernanza de ciberseguridad. Para la prestación de los servicios solicitados se requiere por parte de las empresas la asignación de recursos humanos con un alto nivel de capacitación técnica para resolver los problemas que se planteen de forma satisfactoria, así como la colaboración entre las empresas adjudicatarias para asegurar la calidad y eficacia del servicio.

El objetivo de este Pliego de Prescripciones Técnicas es definir el alcance, así como las características generales y particulares y condiciones de ejecución a las que debe ajustarse el servicio solicitado.

2 OBJETO DEL CONTRATO

El objeto de este expediente es la contratación de servicios de soporte especializado en materia de cumplimiento normativo, gestión de riesgos y gobernanza de la ciberseguridad para la Agencia Vasca de Ciberseguridad.

La prestación de los servicios solicitados requiere la asignación de recursos humanos con un alto nivel de capacitación técnica para resolver los problemas que se planteen de forma satisfactoria. Además, las empresas licitantes deberán proporcionar refuerzo y soporte a las personas asignadas al contrato cuando sea necesario.

La misión de la Oficina Técnica de Seguridad será apoyar a la Agencia en la articulación de sus servicios en materia de cumplimiento normativo, gestión de riesgos y gobernanza de la ciberseguridad para el conjunto de las administraciones públicas de la Comunidad Autónoma Vasca, y en el desarrollo de los modelos necesarios para potenciar y coordinar el alineamiento de la ciberseguridad en dicho conjunto.

El contrato se divide en tres lotes, que corresponden a los ámbitos del cumplimiento normativo, la gestión de riesgos y la gobernanza de la ciberseguridad. Sin embargo, es necesaria la colaboración entre las empresas adjudicatarias de los distintos lotes, ya que estas áreas están interrelacionadas y requieren una visión conjunta y coherente. Esta colaboración será una obligación de las empresas adjudicatarias, y será supervisada por la Agencia, que promoverá la coordinación entre las empresas contratadas para asegurar la calidad y eficacia del servicio prestado.

Los objetivos a conseguir en cada uno de los lotes son los siguientes:

- Lote 1 – Cumplimiento Normativo
  - Proporcionar un servicio integral en el ámbito del cumplimiento normativo en ciberseguridad.
  - Asistir a la Agencia en el cumplimiento de normativas y estándares como el GDPR, Esquema Nacional de Seguridad o la ISO 27001.
  - Diagnosticar el nivel de cumplimiento normativo en el sector público vasco.
  - Prestar asistencia en el desarrollo y supervisión de planes, guías, normas y directrices de ciberseguridad.

- Lote 2 – Gestión de Riesgos
  - Desarrollar un modelo de medición del riesgo aplicable en los tres niveles de administraciones públicas vascas y servicios esenciales.
  - Adaptar el modelo a los cambios en el entorno de la organización y el panorama de amenazas.
  - Apoyar en el tratamiento de los riesgos.
  - Capturar datos pertinentes para evaluar el nivel de riesgo de las organizaciones.

- Lote 3 – Gobernanza de la Ciberseguridad
  - Desarrollar un modelo de ciberseguridad común basado en estándares y marcos de referencia reconocidos.
  - Adaptar el modelo a las necesidades específicas del sector público vasco y desarrollar materiales tipo para facilitar su despliegue.
  - Asistir a la Agencia en establecer y mantener un marco de gobernanza de la ciberseguridad que coordine la actuación del sector público en esta materia.
  - Definir y mantener un cuadro de mando que proporcione una visión cuantitativa del estado de la seguridad en Euskadi.

3 TAREAS A REALIZAR

3.1 LOTE 1 – Cumplimiento Normativo

La empresa adjudicataria de este lote deberá ofrecer un servicio integral en el ámbito del cumplimiento normativo en materia de ciberseguridad.

En primer lugar, la empresa adjudicataria deberá **ayudar a la Agencia a cumplir con las normativas** y estándares de seguridad de la información relevantes. Esto puede incluir normativas como el Reglamento General de Protección de Datos (GDPR), estándares como la ISO 27001 o el Esquema Nacional de Seguridad. El servicio incluirá la elaboración de los planes de adecuación, así como la elaboración de la documentación requerida por la Agencia en esta materia.

La empresa adjudicataria deberá tener un profundo conocimiento de las normativas y estándares relevantes, y deberá ser capaz de interpretar y aplicar estos requisitos al contexto específico de la organización. Esto implicará entender no solo el texto de las normativas y estándares, sino también su espíritu y su propósito.

Además, la empresa adjudicataria deberá apoyar a la Agencia en mantener su cumplimiento a lo largo del tiempo. Esto implicará la monitorización continua de los cambios en las normativas y estándares, así como de los cambios en el entorno de la organización que podrían afectar a su cumplimiento. También implicará la realización de evaluaciones de cumplimiento periódicas para verificar que la Agencia sigue cumpliendo con sus obligaciones.

Por otro lado, la empresa adjudicataria asistirá a la Agencia en el **diagnóstico del nivel de cumplimiento normativo de ciberseguridad en el ámbito del sector público vasco**. De esta manera determinará en qué medida las organizaciones públicas de Euskadi cumplen con las normativas o estándares de referencia. Esto podría implicar la realización de análisis GAP o evaluaciones de cumplimiento. Será responsabilidad del servicio proponer los métodos de evaluación más adecuados en cada caso, que deberán adecuarse al esquema objeto de evaluación.

Si se identifican áreas de no cumplimiento, la empresa adjudicataria propondrá a las organizaciones la implementación de las medidas correctivas necesarias para alcanzar el cumplimiento. Las medias podrían incluir actuaciones como la revisión y actualización de las políticas y procedimientos de seguridad, la implementación de nuevos controles de seguridad, o la formación de los empleados en las obligaciones de cumplimiento.

Así mismo, la empresa adjudicataria asesorará en materia de cumplimiento normativo de ciberseguridad a aquellas organizaciones del sector público vasco que así lo requieran. Esto podría implicar actividades como el asesoramiento sobre la aplicación y el cumplimiento de normativas específicas o la propuesta de recomendaciones técnicas para implementar controles de seguridad.

Por último, la empresa adjudicataria asistirá a la Agencia en el **desarrollo de normas y directrices de ciberseguridad**. Dentro de esta actividad se incluirá la elaboración de materiales como un plan de apoyo en ciberseguridad y de planes específicos de respuesta para los sectores esenciales, con el fin de abordar incidentes que puedan tener un impacto significativo en varios operadores de un mismo sector.

Así mismo, la empresa adjudicataria participará en la supervisión de los planes de continuidad en materia de ciberseguridad de aquellas actividades, centros, establecimientos o infraestructuras a las que les aplique la obligatoriedad de autoprotección en la Norma Vasca de Autoprotección, y cuya actividad se desarrolle dentro de determinados sectores. Esto podría implicar la supervisión e inspección de los planes de continuidad, la resolución de las dudas que los titulares de las actividades

puedan trasladar a la Agencia o el desarrollo de guías para la elaboración de los planes de continuidad en materia de ciberseguridad.

La adjudicataria apoyará a la Agencia en el desarrollo y supervisión de planes, estándares y directrices adicionales en materia de ciberseguridad, que vayan más allá de los descritos en el presente apartado.

3.2 LOTE 2 – Gestión de Riesgos

La empresa adjudicataria de este lote deberá ofrecer un servicio integral para la gestión de riesgos de ciberseguridad.

El servicio comenzará con la asistencia en el desarrollo de un **modelo de medición del riesgo** que será de aplicación en los tres niveles de administraciones públicas vascas y servicios esenciales. El modelo deberá estar basado en modelos de referencia, pero a su vez deberá ser personalizado para reflejar las necesidades y circunstancias específicas del conjunto de las administraciones públicas de Euskadi.

El modelo de medición del riesgo deberá proporcionar una cuantificación objetiva y reproducible del riesgo. Deberá tener en cuenta tanto la probabilidad como el impacto de los riesgos, y deberá ser capaz de acomodar una amplia gama de tipos de riesgos, desde riesgos técnicos, como los asociados con las vulnerabilidades del software, hasta riesgos organizativos, como los asociados con el comportamiento humano. La probabilidad se refiere a la frecuencia con la que se espera que ocurra un evento de riesgo, mientras que el impacto se refiere a la magnitud del daño que podría causar el evento.

El modelo de medición del riesgo también deberá ser dinámico, es decir, deberá ser capaz de adaptarse a medida que cambian las circunstancias de la organización y el panorama de amenazas. Esto podría implicar la recalibración periódica del modelo, así como la incorporación de nuevos tipos de riesgos a medida que se identifican.

Así mismo, el modelo de medición del riesgo deberá ser transparente y comprensible para los usuarios no técnicos. Esto significa que los resultados del modelo deberán ser presentados de una manera que sea fácil de entender, incluso para las personas que no tienen un conocimiento profundo de la seguridad de la información.

Una vez desarrollado el modelo, la empresa adjudicataria apoyará a la Agencia en el **tratamiento de los riesgos** y en la recogida de los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en Euskadi. El objetivo de esta captura será evaluar el nivel de riesgo de las organizaciones de acuerdo con el modelo definido.

Esta evaluación ayudará a las organizaciones a priorizar sus esfuerzos de mitigación y a asignar recursos de manera eficiente. Adicionalmente, la adjudicataria propondrá las acciones necesarias para mitigar los riesgos identificados. Estas acciones podrían incluir planes formativos o la definición de controles cuya implementación permita reducir la probabilidad o el impacto de los riesgos.

3.3 LOTE 3 – Gobernanza de la ciberseguridad

La empresa adjudicataria de este lote deberá ofrecer un servicio integral en el ámbito de la gobernanza de ciberseguridad.

El servicio comenzará con la asistencia en el desarrollo de un **modelo de ciberseguridad** común que será de aplicación en los tres niveles de administraciones públicas de Euskadi. Su propósito será desarrollar un marco de directrices y normas técnicas recomendables para el sector público vasco en el ámbito de la ciberseguridad. El modelo deberá estar basado en estándares de seguridad reconocidos, como la ISO 27001 o el ENS, pero deberá ser personalizado y detallado para reflejar las necesidades y circunstancias específicas del conjunto de las administraciones públicas de Euskadi.

El modelo incluirá principios básicos que guíen las decisiones de seguridad de las organizaciones, requisitos específicos que las organizaciones deban cumplir y medidas de seguridad que las organizaciones deban implementar. Estas medidas podrían incluir controles técnicos, como firewalls o software antivirus; controles operativos, como la gestión de vulnerabilidades; y controles organizativos, como políticas de seguridad o procedimientos.

La aplicación del modelo deberá garantizar, al menos, la identificación de los activos críticos de la organización, la definición de los controles de seguridad necesarios para proteger dichos activos y la evaluación exhaustiva de la postura de ciberseguridad de cada organización.

Para facilitar el **despliegue del modelo** la empresa adjudicataria desarrollará los materiales tipo que permitan articular el modelo de ciberseguridad diseñado. Este es un paso crucial en el proceso, ya que estos materiales servirán como base para la implementación del modelo en las diferentes administraciones públicas de Euskadi. Los materiales tipo podrían incluir guías de implementación, plantillas de políticas de seguridad, listas de verificación de cumplimiento, entre otros recursos útiles. Estos materiales serán diseñados de manera que sean fácilmente comprensibles y aplicables, independientemente del tamaño o la capacidad técnica de la organización.

Además, la empresa adjudicataria apoyará a la Agencia en la difusión del modelo y de los materiales tipo, con el objetivo de promover la adopción del modelo en el sector público vasco. Esto podría implicar la realización de talleres de formación y otras actividades de divulgación para asegurar que las organizaciones comprendan el modelo y cómo implementarlo. El servicio incluirá también el acompañamiento individualizado en aquellas organizaciones que la Agencia determine. Este acompañamiento podría incluir un asesoramiento técnico o la recogida de datos para impulsar la implementación del modelo.

Por otro lado, la empresa adjudicataria asistirá a la Agencia en el establecimiento y mantenimiento de un **marco de gobernanza de la ciberseguridad** que permita coordinar la actuación del sector público en materia de ciberseguridad, con una perspectiva de país.

Para ello se modelará un sistema de gobernanza que defina claramente los roles y responsabilidades en relación con la ciberseguridad. De igual forma, se definirán la estructura y las políticas necesarias para coordinar la ciberseguridad del sector público de Euskadi desde una perspectiva transversal, con el objetivo de optimizar y mejorar la eficiencia de los recursos existentes.

Finalmente, se definirán los indicadores clave de rendimiento (KPIs) y métricas de seguridad que permitan a la Agencia supervisar la efectividad de los modelos de ciberseguridad, gobernanza y medición del riesgo, así como del nivel de cumplimiento normativo en el ámbito de la ciberseguridad para el conjunto de administraciones públicas de Euskadi.

La adjudicataria integrará estos indicadores en un **cuadro de mando** que proporcione una visión cuantitativa del estado de la seguridad en el sector público de Euskadi. El mantenimiento del cuadro de mando y la recogida de los indicadores clave de rendimiento (KPIs) y métricas de seguridad será responsabilidad de la empresa adjudicataria.

Adicionalmente, la Agencia podrá requerir que el cuadro de mando incluya algún tipo de información generada desde otros servicios de la Agencia.

4 DEFINICIÓN DEL SERVICIO

4.1 Fases del servicio

Se identifican las siguientes fases:

4.1.1 Periodo de transición

El periodo de transición tendrá una duración máxima de dos semanas y consiste en el tiempo necesario para poner en marcha la Oficina Técnica de Seguridad, debe incluir la recepción de los elementos básicos por parte de la Agencia Vasca de Ciberseguridad y el personal de la empresa adjudicataria. Durante esta fase, se asignarán roles, tareas y responsabilidades, y se elaborará un plan detallado de actividades y un plan de activación del servicio, que serán revisados y validados por la Agencia. Una vez finalizada la fase de transición, se procederá al inicio de la prestación regular del servicio.

4.1.2 Prestación regular del servicio

La fase de servicio regular comenzará a la finalización de la fase de transición y finalizará con el inicio de la fase de devolución del servicio.

Desde el inicio del servicio, el personal de la empresa adjudicataria deberá funcionar de manera autónoma, resolviendo adecuadamente y en los plazos marcados las peticiones de trabajo que se le encomienden, gestionando los recursos y obteniendo los indicadores e informes establecidos para las reuniones de seguimiento.

Por parte de la Agencia se podrán especificar herramientas concretas en las que se desea se reporte parte o toda la información relativa a los indicadores anteriormente mencionados.

4.1.3 Devolución

La empresa adjudicataria estará obligada a prestar apoyo, y realizar la transferencia de conocimiento, documentación, etc. a la siguiente empresa adjudicataria del contrato, en caso de que esta sea distinta a la empresa adjudicataria del presente pliego.

El plazo máximo para la fase de devolución no será superior a dos semanas. Esta fase de salida deberá llevarse a cabo tras la finalización del período del presente contrato o su prórroga sin costo adicional para la Agencia.

4.2 Entregables

La empresa adjudicataria de cada lote proporcionará mensualmente informes de seguimiento del servicio, con información sobre la dedicación, tareas y entregables del período.

En relación con los entregables del periodo, la oferta contendrá un plan de entregables, incluyendo una descripción detallada de su contenido.

Además, se requiere que todos los entregables del proyecto se entreguen en formato bilingüe, es decir, en euskera y castellano, respetando la calidad lingüística y técnica de ambos idiomas. La empresa adjudicataria deberá contar con personal cualificado para realizar las traducciones necesarias y garantizar la coherencia terminológica y conceptual entre las dos versiones. Asimismo, los entregables se elaborarán siguiendo las plantillas de documentación indicadas por la Agencia,

que contendrán el formato y el estilo adecuados para cada tipo de documento. La empresa adjudicataria deberá adaptarse a las posibles modificaciones o actualizaciones de las plantillas que la Agencia pueda realizar durante la ejecución del contrato.

A continuación, se incluyen algunos ejemplos de posibles entregables. En cualquier caso, los entregables aquí detallados se deben considerar como una primera aproximación. La adjudicataria de cada lote deberá acordar con la Agencia cada uno de los entregables a generar, así como el contenido detallado de cada uno de ellos, con el objetivo de garantizar la calidad final del servicio realizado.

- **Ejemplos para el Lote 1 – Cumplimiento Normativo:**
  - Resultados de los diagnósticos realizados en el periodo.
  - Evaluación del estado actual de cumplimiento.
  - Plan de acción para el cumplimiento de las normativas aplicables.
  - Informes periódicos de cumplimiento.
  - Análisis de los requisitos legales y regulatorios aplicables.
  - Cualesquiera otros que la empresa licitadora considere necesarios.

- **Ejemplos para Lote 2 – Gestión de Riesgos:**
  - Modelo de medición del riesgo.
  - Resultados de las evaluaciones de medición del riesgo.
  - Plan de acción para la mitigación de riesgos.
  - Informes periódicos de seguimiento de riesgos.
  - Cualesquiera otros que la empresa licitadora considere necesarios.

- **Ejemplos para Lote 3 – Gobernanza de la Ciberseguridad:**
  - Modelo de ciberseguridad común.
  - Marco de gobernanza de la ciberseguridad.
  - Informes de estado de la ciberseguridad.
  - Políticas y procedimientos de ciberseguridad.
  - Cuadro de mando de indicadores.
  - Cualesquiera otros que la empresa licitadora considere necesarios.

En cualquier caso y aplicado a todos los lotes objeto del expediente, toda la documentación, publicidad, imagen o material que se genere con motivo de la ejecución del contrato, la empresa o entidad adjudicataria deberá emplear un uso no sexista del lenguaje, evitar cualquier imagen discriminatoria de las mujeres o estereotipos sexistas y fomentar una imagen con valores de igualdad, presencia equilibrada, diversidad, corresponsabilidad y pluralidad de roles e identidades de género.

4.3 Modelo de prestación del servicio

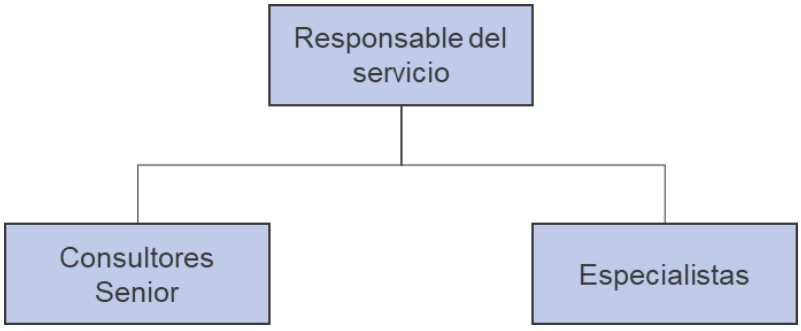
Debido a la naturaleza sensible de la información que se va a gestionar dentro del alcance del contrato, el acceso a los sistemas y la necesidad de coordinación con otras áreas de Cyberzaintza, se hace necesario que el equipo realice la actividad en los siguientes términos:

- Las reuniones mensuales de seguimiento se llevarán a cabo exclusivamente de manera presencial en las oficinas de Cyberzaintza y será necesaria la asistencia del Responsable del servicio.
- De manera general los perfiles de Especialistas prestarán el servicio en las instalaciones del adjudicatario. Sin perjuicio de que haya ciertas circunstancias en las que la Agencia solicite la presencia de uno o varios miembros del equipo de trabajo en sus oficinas. Estas situaciones pueden surgir debido a la criticidad de los trabajos a realizar o a una necesidad puntual de la Agencia.
- Los Consultores Senior prestarán el servicio en las instalaciones del adjudicatario, con la realización de actividades de manera presencial en las instalaciones de Cyberzaintza al menos dos días a la semana. Los días específicos para trabajar físicamente en la oficina serán acordados con el responsable del servicio, y en caso de desacuerdo, la Agencia determinará los días correspondientes. Además, puede haber ocasiones en las que la Agencia solicite una presencia física más frecuente debido a la importancia crítica de las tareas a realizar o por necesidades puntuales.
- En función de las necesidades del servicio podrá ser necesaria la presencia del equipo de trabajo en otras ubicaciones (alcance geográfico de País Vasco) como, por ejemplo, evaluaciones, recogida de datos, sesiones de acompañamiento o reuniones en distintos organismos vinculados con la Agencia.

El adjudicatario asumirá los gastos derivados de los desplazamientos, dietas y otros costos asociados a la disposición de medios necesarios para estos y, en general, para la ejecución del proyecto en las condiciones de presencialidad indicadas. A efectos de realizar la propuesta, se estiman 10 desplazamientos mensuales fuera de las instalaciones de Cyberzaintza. No obstante, es importante señalar que esta cifra no es vinculante y puede cambiar según las necesidades y circunstancias específicas de la Agencia.

4.4 Equipo de trabajo

Para cada uno de los lotes el equipo de trabajo encargado de construir el entorno objeto de este contrato deberá respetar el siguiente organigrama:



Responsable del servicio

La persona con rol de Responsable del servicio será la encargada de ejercer las facultades de responsable en lo referente al servicio contratado y de gestionar cualquier problema o incidente importante que pueda surgir. Así mismo, se responsabilizará frente a la Agencia de las personas que prestan el servicio.

A continuación, se detallan los requisitos mínimos que deberán cumplir las personas que tengan rol de Responsable del servicio:

- Contar con más de 10 años de experiencia en el sector de la Ciberseguridad, siendo al menos los 7 últimos en dicho sector.
- Experiencia acreditada como coordinador durante los últimos 5 años.

Consultores Senior

Las personas con rol de Consultor Senior tendrán categoría de consultor senior, con experiencia en la realización de tareas similares a las descritas para el lote correspondiente. Se responsabilizarán de las actividades cotidianas del servicio, pudiendo consultar a los especialistas cuando se enfrenten a tareas que requieran un conocimiento más especializado.

A continuación, se detallan los requisitos mínimos que deberán cumplir las personas que tengan rol de Consultor Senior:

- Contar con más de 5 años de experiencia en el sector de la Ciberseguridad, siendo al menos los 3 últimos en dicho sector.
- Experiencia acreditada como consultor GRC durante los últimos 3 años.

Especialistas

Las personas con rol de Especialista proporcionarán asesoramiento experto en su área de especialización a los consultores senior que presten el servicio con dedicación exclusiva para la Agencia. Además, tendrán un papel activo en la toma de decisiones estratégicas dentro del contexto del servicio.

A continuación, se detallan los requisitos mínimos que deberán cumplir las personas que tengan rol de Especialistas:

- Contar con más de 7 años de experiencia en el sector de la Ciberseguridad, siendo al menos los 5 últimos en dicho sector.
- Experiencia acreditada como consultor GRC durante los últimos 5 años.

4.5 Dimensionamiento y dedicación

Las propuestas deben dimensionar los recursos necesarios para prestar el servicio, cumpliendo todos los requisitos. No obstante, se establece como requisito mínimo que el equipo disponga de la capacidad especificada en la tabla siguiente para cada uno de los roles, garantizando la dedicación indicada durante la ejecución del contrato.

LOTE 1 – Cumplimiento Normativo

	Dedicación (%)	Año 1	Total	Formato
Responsable del servicio	**5%**	85 horas	**170 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Especialistas	**30%**	510 horas	**1.020 horas**	Bolsa de horas (consumo bajo demanda)

LOTE 2 – Gestión de Riesgos

	Dedicación (%)	Año 1	Total	Formato
Responsable del servicio	**5%**	85 horas	**170 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Especialistas	**30%**	510 horas	**1.020 horas**	Bolsa de horas (consumo bajo demanda)

LOTE 3 – Gobernanza de la ciberseguridad

	Dedicación (%)	Año 1	Total	Formato
Responsable del servicio	**5%**	85 horas	**170 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Consultor Senior	**100%**	1.700 horas	**1.700 horas**	Recurso nominal
Especialistas	**30%**	510 horas	**1.020 horas**	Bolsa de horas (consumo bajo demanda)

5 EJECUCIÓN DEL CONTRATO

La empresa adjudicataria será responsable del correcto desarrollo de los trabajos y proyectos relacionados, de acuerdo a los requerimientos del presente pliego.

5.1 Supervisión del contrato

La actuación de la empresa adjudicataria será supervisada por la persona responsable que la Agencia Vasca de Ciberseguridad designe. Asimismo, la empresa adjudicataria designará a una persona Responsable del Servicio, con dedicación estable y adecuada, quien será responsable de coordinar las tareas del servicio y servirá como interlocutora principal con la dirección del proyecto de la Agencia.

Deberán establecerse todos los mecanismos de control que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en plazos como en términos de calidad final. Para ello se contempla:

- Reuniones de seguimiento: periódicamente se celebrarán reuniones destinadas a revisar el grado de cumplimiento de las tareas planificadas, las programaciones de actividades a realizar, etc.
- Informes de situación y progreso: con los que la empresa adjudicataria comunicará a la dirección del proyecto el estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc. Estos informes deberán quedar adecuadamente registrados y formalizados.
- Documentos de gestión de proyectos/servicios: la empresa adjudicataria cumplimentará los documentos de gestión de proyectos/servicios, según un modelo definido (actas de reuniones, informes de progreso, etc.
- Entregables: puesto que se propone un proceso iterativo de entregas, periódicamente se entregarán los productos obtenidos (documentación, código, etc.) obtenidos con independencia de su calificación de “definitivos” o no.

Horario del servicio

Para la ejecución de las tareas especificadas en este contrato, se requiere que la empresa adjudicataria disponga del personal necesario al menos durante la jornada laboral, independientemente de si los trabajos se realizan de forma presencial o mediante teletrabajo. En su oferta, la empresa licitadora deberá especificar los horarios correspondientes a la jornada laboral del año natural.

Asimismo, la empresa adjudicataria debe proporcionar al menos un número de teléfono y una dirección de correo electrónico para contactar con el personal asignado al servicio, garantizando que dicho contacto estará disponible en todo momento durante el horario establecido.

5.2 Asignación del Personal

Los perfiles propuestos para prestación del servicio deben ser nominales de personal de la empresa, **no admitiéndose perfiles genéricos**. La empresa licitadora deberá aportar el detalle de las cualificaciones profesionales del equipo propuesto para la prestación del servicio. Con este propósito, deberá cumplimentar y presentar como anexo de la memoria técnica la tabla detallada en el documento EquipoTrabajo.xlsx.

Es requisito que dicha tabla se incluya en formato EXCEL.

Las certificaciones y cursos indicados en la tabla "EquipoTrabajo.xlsx" se deberán declarar y posteriormente acreditar.

La empresa licitadora se compromete, en caso de ser adjudicataria, a mantener el equipo, según lo establecido en el documento de Propuesta Técnica, y durante el periodo fijado en cada actividad específica. Los recursos asignados a la ejecución del contrato deberán estar asignados desde el inicio del mismo. En el caso de modificación o sustitución de recursos, deberá comunicarlo previamente a la Agencia, con la antelación necesaria en función de la criticidad del servicio, y en cualquier caso al menos 15 días naturales previos a la realización del cambio de recurso, y la Agencia aprobará o rechazará dicha modificación o sustitución. En todo caso el sustituto o sustitutos tendrán un perfil igual o superior al ofertado, o recurso a sustituir.

La Agencia podrá solicitar el cambio de los recursos asignado a los servicios, por inadecuación de los recursos o por incumplir los requisitos tanto de solvencia como técnicos exigidos, o haber declarado el contratista unas circunstancias que no son veraces, en cuyo caso podrá conllevar la rescisión del contrato y adjudicación al licitador siguiente en las calificaciones.

5.2.1 Constitución inicial del equipo de trabajo

El equipo técnico a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por componentes y perfiles relacionados en la oferta adjudicataria y consecuentemente valorados.

Si tras la adjudicación se observara que el equipo de proyecto no se corresponde con el establecido en la oferta técnica y:

- Caso que el adjudicatario presente justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio, se procederá a:
  - La presentación por el adjudicatario de sustituto/a con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
  - Aceptación del sustituto/a por parte del responsable del servicio de la Agencia.
- Caso de que se demostrase que el cambio no se corresponde con causa justificada, la Agencia se reserva el derecho no solo a la aprobación del sustituto/a sino incluso a la revisión de la adjudicación y en su caso la rescisión del pedido/contrato, si este hecho fuera elemento determinante en la mencionada adjudicación.

5.2.2 Modificaciones en la composición del equipo de trabajo

Si la empresa adjudicataria propusiera el cambio de alguna de las personas del equipo de trabajo, se deberá solicitar por escrito con quince días naturales de antelación, y requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de sustituto/a con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación del sustituto/a por parte del responsable del servicio de la Agencia.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones de personal, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario. Si a criterio de la persona responsable del servicio de la Agencia, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/a no serán facturables corriendo a cargo de la empresa adjudicataria.

No obstante, la designación de las personas que componen el Equipo de Trabajo realizada por la empresa adjudicataria podrá ser modificada, a simple petición de la Agencia, y en este caso, la empresa adjudicataria se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por la Agencia de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

5.3 Registro y Control

Como parte del contrato, la empresa adjudicataria estará obligada a dar total cumplimiento a las condiciones que al efecto de control establezca la Agencia.

La empresa adjudicataria deberá proporcionar la información requerida por la Agencia para conocer la situación y desarrollo de los trabajos contratados.

Durante la ejecución del contrato la Agencia se reserva el derecho de verificar la corrección de la prestación y adecuación de la misma a los pliegos de cláusulas administrativas, a este pliego de prescripciones técnicas y a la oferta de la empresa adjudicataria. En tal sentido la empresa adjudicataria deberá proceder dentro del plazo que se indique a la subsanación o reajuste de los extremos que hayan sido puestos de relieve.

El incumplimiento por parte de la empresa adjudicataria de lo establecido en el presente pliego de Bases Técnicas y cuando dicho incumplimiento sea reiterativo o se refiera a órdenes que le hayan sido impartidas por escrito y advirtiéndole que son esenciales para el buen fin del contrato, se considerará causa de resolución del mismo.

6 SEGURIDAD

6.1 Secreto y Confidencialidad

La empresa contratista debe observar estrictamente las obligaciones de secreto y confidencialidad de cualquier información relativa a la ejecución de este contrato. Todos los trabajos que se realicen con ocasión de este contrato tienen carácter secreto y confidencial, por lo que la empresa contratista no podrá usar para sí, ni proporcionar a terceros, datos o información alguna relativa al mismo, ni tampoco ninguna referencia a la documentación facilitada por la Agencia Vasca de Ciberseguridad. La empresa contratista queda obligada a poner todos los medios a su alcance para preservar el secreto y confidencialidad de la información a la que tenga acceso durante la ejecución del contrato.

6.2 Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán a la Agencia Vasca De Ciberseguridad. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito de la Agencia Vasca De Ciberseguridad.

Asimismo, todos los entregables que deban facilitarse a la Agencia Vasca De Ciberseguridad (salvo los relativos a las ofertas del procedimiento de licitación) únicamente deberán llevar como logotipo o señas de identidad el escudo del Gobierno Vasco o logotipos aceptados por la propia Agencia Vasca De Ciberseguridad.

La empresa contratista se verá también obligada a guardar las normas vigentes sobre Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vea obligado a manejar.

Al finalizar el contrato, una vez haya sido transferida la información a la Agencia Vasca De Ciberseguridad, la empresa contratista se compromete a su destrucción, teniendo en cuenta los distintos soportes o documentos donde esta pueda constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc. A tal efecto, una vez realizada la operación descrita, entregará una declaración firmada a la Agencia Vasca De Ciberseguridad donde conste que así se ha realizado.