Expediente: “ACUERDO MARCO PARA LA REALIZACIÓN DE AUDITORÍAS PARA EL ÓRGANO DE AUDITORÍA TÉCNICA DE LA AGENCIA VASCA DE CIBERSEGURIDAD”

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Índice

1 INTRODUCCIÓN 4
2 OBJETO DEL CONTRATO 5
3 TAREAS A REALIZAR 6
3.1 LOTE 1 – Auditorías de conformidad 6
3.1.1 Fase preliminar: Generación de la necesidad 6
3.1.2 Fase inicial: Selección de la empresa auditora 7
3.1.3 Segunda fase: Planificación de la auditoría y selección de la empresa revisora del expediente 7
3.1.4 Tercera fase: Lanzamiento de la auditoría 8
3.1.5 Cuarta fase: Ejecución de la auditoría 9
3.1.6 Quinta fase: Revisión de la auditoría 9
3.1.7 Sexta fase: Auditoría extraordinaria 10
3.2 LOTE 2 – Auditoría interna 10
3.2.1 Fase preliminar: Establecimiento del programa de auditoría 10
3.2.2 Primera fase: Planificación de las auditorías internas 11
3.2.3 Segunda fase: Lanzamiento de la auditoría 11
3.2.4 Tercera fase: Ejecución de la auditoría 11
3.2.5 Cuarta fase: Auditoría extraordinaria 12
4 DEFINICIÓN DEL SERVICIO 13
4.1 Fases del servicio 13
4.1.1 Preparación del servicio 13
4.1.2 Prestación regular del servicio 13
4.1.3 Devolución 14
4.2 Entregables 14
4.3 Modelo de prestación del servicio 15
4.4 Equipo de trabajo 15
4.4.1 Responsable del servicio 15
4.4.2 Auditores 16
4.5 Dimensionamiento y dedicación 16
5 EJECUCIÓN DEL CONTRATO 18
5.1 Supervisión del contrato 18
5.2 Horario del servicio 18

5.3 Asignación del Personal 18
5.3.1 Constitución inicial del equipo de trabajo 19
5.3.2 Modificaciones en la composición del equipo de trabajo 19
5.4 Registro y Control 19
6 SEGURIDAD 21
6.1 Secreto y Confidencialidad 21
6.2 Ausencia de conflictos de interés 21
6.3 Propiedad intelectual 21

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, tal y como establece la Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad. 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.

Así mismo, los Estatutos de la Agencia Vasca de Ciberseguridad, aprobados a través del Decreto 34/2024, de 19 de marzo, determinan, entre otros, su objeto, funciones y principios generales de actuación. Éstos, a su vez, fueron modificados mediante el Decreto 15/2026, de 17 de febrero, de modificación del Decreto por el que se aprueban los Estatutos de la Agencia Vasca de Ciberseguridad, con el objeto de incorporar, entre las funciones de la Agencia, la auditoría de sistemas de información, dando así cumplimiento a la obligación de realizar auditorías periódicas establecida en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

Recogiendo la iniciativa planteada por el Consejo de Administración de la Agencia, Cyberzaintza se constituyó como Órgano de Auditoría Técnica (en adelante, OAT) para la certificación de la conformidad del ENS, de acuerdo con lo establecido en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, y en la Guía CCN-STIC 122 que establece el procedimiento de reconocimiento y los requisitos que debe cumplir un Órgano de Auditoría Técnica del ENS, obteniendo el correspondiente reconocimiento el 13 de mayo de 2026.

Considerando dicha constitución como OAT, la Agencia Vasca de Ciberseguridad necesita contratar servicios de auditoría del ENS que puedan ampliar y completar las capacidades de la Agencia en relación con la certificación de la conformidad con el ENS, con el fin de contribuir a asentar las capacidades desarrolladas y a mejorar las garantías de imparcialidad, independencia y ausencia de conflictos de interés ofrecidas por la Agencia.

El contrato se divide en dos lotes: uno específico para la ejecución de las auditorías de conformidad con el ENS y la revisión de los expedientes relativos a dichas auditorías de conformidad, y un segundo para la auditoría interna del propio OAT. Para la prestación de dichos servicios se requiere por parte de las empresas licitadoras la asignación de recursos humanos con un alto nivel de capacitación técnica para llevar a cabo las tareas correspondientes 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 auditoría y revisión para la certificación de la conformidad con el Esquema Nacional de Seguridad.

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

La misión del servicio de auditorías será la de apoyar al Órgano de Auditoría Técnica de la Agencia en la articulación de sus servicios en materia de certificación de la conformidad con el ENS dentro de su ámbito competencial, así como en todo lo relativo a la auditoría interna del propio funcionamiento como OAT.

El contrato se divide en dos lotes, que corresponden con las diferentes funciones en las que el OAT necesita asistencia especializada:

- La ejecución de las auditorías de conformidad con el ENS y la revisión de los expedientes correspondientes a dichas auditorías.
- La auditoría interna del propio OAT.

No obstante, es imprescindible que dicha asistencia se lleve a cabo garantizando por un lado la necesaria coordinación y complementariedad de dichas actividades y por otro la imprescindible independencia y ausencia de conflictos de interés entre todas ellas. Por este motivo, será labor del Órgano de Auditoría Técnica de la Agencia la correspondiente coordinación y supervisión de todas las actividades, con el fin de garantizar la necesaria complementariedad entre las empresas contratadas y la calidad y eficacia del servicio prestado.

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

- Lote 1 – Auditorías de conformidad
  - Proporcionar toda la capacidad necesaria para la realización de auditorías de certificación de la conformidad con el ENS en cualquiera de sus categorías, niveles o perfiles de cumplimiento, satisfaciendo todos los requisitos aplicables.
  - Proporcionar toda la capacidad necesaria para revisar, de manera totalmente independiente, las auditorías de certificación de la conformidad con el ENS realizadas, satisfaciendo todos los requisitos aplicables.
  - Proporcionar un dimensionamiento adecuado del servicio para que dicha capacidad se pueda poner en práctica en los tiempos y formas requeridos por el OAT.
- Lote 2 – Auditoría interna
  - Proporcionar toda la capacidad necesaria para evaluar, de manera totalmente independiente a los procesos anteriores, la correcta aplicación de las prácticas y criterios necesarios para llevar a cabo la certificación de la conformidad con el ENS de manera adecuada y garantizando en todo momento la necesaria imparcialidad, independencia y ausencia de conflictos de interés.
  - Proporcionar un dimensionamiento adecuado del servicio para que dicha capacidad se pueda poner en práctica en los tiempos y formas requeridos por el OAT.

3 TAREAS A REALIZAR

3.1 LOTE 1 – Auditorías de conformidad

Las empresas adjudicatarias de este lote deberán ofrecer, bajo el modelo de funcionamiento comúnmente conocido como "cesión de auditores", las capacidades necesarias para que el Órgano de Auditoría Técnica de Cyberzaintza pueda llevar a cabo, a través de dichos servicios, las funciones de:

- Auditor jefe
- Auditor
- Revisor de expedientes

Para ello, el modelo de funcionamiento se estructurará de acuerdo con las fases descritas a continuación.

3.1.1 Fase preliminar: Generación de la necesidad

Durante la fase previa a la prestación del servicio por parte de las empresas adjudicatarias, los organismos públicos del País Vasco se pondrán en contacto con el OAT de Cyberzaintza para solicitar sus servicios de certificación de la conformidad con el ENS.

Durante esta fase preliminar, el OAT determinará de forma preliminar, juntamente con el organismo público solicitante:

- El alcance de la auditoría
- La categoría de los sistemas objeto de la auditoría
- Las fechas de referencia planteadas por el organismo público para llevar a cabo la auditoría
- Otros aspectos que puedan ser relevantes para la prestación del servicio:
    - Sede(s)
    - Modalidad de la auditoría (presencial / remota / mixta)
    - Idioma(s) de la auditoría
    - Etc.

Con esa información, la Agencia, en función de las demandas del servicio y de sus capacidades vigentes y previstas, determinará la necesidad de activar los servicios de las empresas adjudicatarias del servicio de auditorías para el OAT para llevar a cabo la auditoría en cuestión. En caso de que se determine dicha necesidad, la Agencia formalizará, de manera preliminar:

- La identidad del organismo público a auditar
- La modalidad de la auditoría y la ubicación de las sedes a visitar, cuando corresponda
- La categoría de los sistemas
- Las funciones que es necesario activar:
    - Auditor jefe
    - Auditores (en cuyo caso, se especificará el número).
- El dimensionamiento preliminar previsto (en jornadas) para cada función.
- Las fechas de referencia planteadas
- Otros condicionantes a considerar

3.1.2 Fase inicial: Selección de la empresa auditora

La información indicada anteriormente se facilitará, inicialmente, a la empresa que más puntos haya logrado en la licitación, indicándose expresamente en dicha comunicación:

- El plazo de planificación considerado
- La consideración de dicho plazo como ordinario o extraordinario
- Toda la información anteriormente recogida

La empresa receptora de dicha comunicación deberá verificar que:

- Está en disposición de ofrecer las capacidades requeridas, con los condicionantes indicados, en las fechas de referencia planteadas.
- No existe, por su parte, ningún conflicto de interés para participar en la realización de la auditoría de dicho organismo público.

En caso de que la empresa que más puntos haya logrado en la licitación confirme su disposición de participar en la auditoría correspondiente, se procederá a la siguiente fase del servicio seleccionando dicha empresa como participante. En caso de que esta empresa rechace el ofrecimiento (por capacidad y/o conflicto de interés), se procederá a proponer dicha participación a la segunda empresa que más puntos haya logrado en la licitación.

En caso de que la segunda empresa que más puntos haya logrado en la licitación confirme su disposición de participar en la auditoría correspondiente, se procederá a la siguiente fase del servicio seleccionando dicha empresa como participante. En caso de que esta empresa también rechace el ofrecimiento, se procederá a proponer dicha participación a la tercera empresa que más puntos haya logrado en la licitación.

En caso de que la tercera empresa que más puntos haya logrado en la licitación confirme su disposición de participar en la auditoría correspondiente, se procederá a la siguiente fase del servicio seleccionando esta empresa como participante. En caso de que ésta también rechace el ofrecimiento, se volverá a la fase preliminar y se revisará la formalización de las necesidades planteadas, con el fin de modificar los parámetros que hayan provocado la imposibilidad de prestar el servicio de acuerdo con el planteamiento original.

3.1.3 Segunda fase: Planificación de la auditoría y selección de la empresa revisora del expediente

Con la empresa adjudicataria que haya aceptado participar en la auditoría de certificación correspondiente se llevará a cabo la planificación detallada de la auditoría. En esta fase se concretarán, mediante el correspondiente diálogo entre todas las partes:

- Los miembros específicos del equipo de trabajo que desempeñarán cada una de las funciones requeridas.
- El número de jornadas específicas que se llevarán a cabo de manera presencial, remota y asíncrona, según corresponda en cada caso.
- Los días específicos que se llevarán a cabo de forma presencial y remota, según corresponda en cada caso.
- El horario en el que se llevarán a cabo las sesiones, tanto presenciales como remotas, cuando corresponda.
- La planificación específica de cada una de las sesiones presenciales y/o remotas, incluyendo todas las consideraciones necesarias.

Así mismo, durante esta fase, la Agencia, en función de las demandas del servicio y de sus capacidades vigentes y previstas, determinará la necesidad de activar los servicios de las empresas adjudicatarias del servicio de auditorías para el OAT para llevar a cabo la revisión del expediente correspondiente a dicha auditoría. En caso de que se determine dicha necesidad, la Agencia formalizará, de manera preliminar:

- La identidad del organismo público a auditar
- La categoría de los sistemas
- La planificación prevista
- El dimensionamiento previsto
- Otros condicionantes que se hayan considerado relevantes

La información indicada anteriormente se facilitará, inicialmente, a la empresa que más puntos haya logrado en la licitación y que no haya sido la empresa a la que se le ha asignado la participación en la auditoría, garantizando de ese modo la total independencia entre ambas funciones. La citada empresa deberá verificar que:

- Está en disposición de ofrecer la capacidad de revisión del expediente, con los condicionantes indicados, en las fechas correspondientes.
- No existe, por su parte, ningún conflicto de interés para participar en la realización de la revisión del expediente de dicho organismo público.

En caso de que la empresa invitada a la prestación del servicio de revisión del expediente confirme su disposición de participar en la auditoría correspondiente, se procederá a la siguiente fase del servicio con dicha empresa como seleccionada en esta función. En caso de que esta empresa rechace el ofrecimiento (por capacidad y/o conflicto de interés), se procederá a proponer dicha participación a la segunda empresa que más puntos haya logrado en la licitación y que no haya sido la empresa a la que se le ha asignado la participación en la auditoría.

Cuando esta segunda empresa confirme su disposición de participar en la auditoría correspondiente, se procederá a la siguiente fase del servicio con dicha empresa como seleccionada para esta función.

3.1.4 Tercera fase: Lanzamiento de la auditoría

En esta fase se llevarán a cabo las firmas, por parte de todo el personal de los equipos de trabajo designados por las correspondientes empresas bien para participar en la ejecución de la auditoría o bien para revisar el expediente correspondiente, de las cláusulas nominales de *confidencialidad* y *ausencia de conflictos de interés*.

La auditoría se organizará y articulará de acuerdo con los procedimientos que el OAT de Cyberzaintza tiene establecidos a tal efecto. Durante esta fase, la labor de la empresa seleccionada para la revisión del expediente será la de verificar que todas las tareas previas se llevan a cabo de acuerdo con los procedimientos establecidos.

En esta fase la empresa seleccionada para la revisión del expediente será la responsable de asegurar la entrega, en tiempo y forma, del correspondiente *Informe de Revisión de Actividades Previas a la Auditoría*.

Si durante esta fase fuese necesario llevar a cabo algún tipo de replanificación o ajuste, dichas tareas se llevarán a cabo juntamente con la empresa seleccionada para la ejecución de la auditoría.

En esta fase, si la empresa ha sido seleccionada para el desarrollo de la función de auditor jefe, ésta será la responsable de asegurar la entrega, en tiempo y forma, del correspondiente *Plan de Auditoría*.

3.1.5 Cuarta fase: Ejecución de la auditoría

La auditoría se desarrollará de acuerdo con los procedimientos que el OAT de Cyberzaintza tiene establecidos a tal efecto. Durante esta fase, la labor de la empresa seleccionada para la ejecución de la auditoría será la de desarrollar las funciones de auditor jefe y/o auditor previstas.

La fase de ejecución de la auditoría contemplará, de acuerdo con dichos procedimientos:

- La propia ejecución de la auditoría
- La generación del informe de auditoría correspondiente
- La evaluación del PAC, si fuese necesario.
- La recomendación final

En esta fase, si la empresa ha sido seleccionada para el desarrollo de la función de auditor jefe, ésta será la responsable de asegurar la entrega, en tiempo y forma, de los correspondientes *Informe de Auditoría y Recomendación del Auditor Jefe al Comité de Certificación*.

Durante esta fase no será necesaria la participación de la empresa seleccionada para la revisión del expediente.

3.1.6 Quinta fase: Revisión de la auditoría

La revisión de la auditoría se desarrollará de acuerdo con los procedimientos que el OAT de Cyberzaintza tiene establecidos a tal efecto. Durante esta fase, la labor de la empresa seleccionada para la revisión del expediente será la de participar en las tareas de:

- La revisión de la auditoría llevada a cabo
- La emisión del certificado

En esta fase la empresa seleccionada para la revisión del expediente será la responsable de asegurar la entrega, en tiempo y forma, del correspondiente *Informe de Revisión del expediente*. Así mismo, deberá colaborar en la elaboración del documento de *Adopción de decisión de certificación*.

Durante esta fase no será necesaria la participación de la empresa seleccionada para la ejecución de la auditoría.

Esta fase finalizará, de manera natural, con la emisión del correspondiente certificado de conformidad con el ENS al organismo público solicitante.

3.1.7 Sexta fase: Auditoría extraordinaria

En caso de que el proceso de auditoría del organismo público solicitante requiera el desarrollo de una auditoría extraordinaria, la empresa seleccionada para la ejecución de la auditoría deberá participar, desarrollando las mismas funciones que en la auditoría ordinaria, en:

- La “planificación de la auditoría” extraordinaria.
- El “lanzamiento de la auditoría” extraordinaria.
- La “ejecución de la auditoría” extraordinaria.

En caso de que el proceso de auditoría del organismo público solicitante requiera el desarrollo de una auditoría extraordinaria, la empresa seleccionada para la revisión del expediente deberá participar, desarrollando las mismas funciones que en la auditoría ordinaria, en:

- El “lanzamiento de la auditoría” extraordinaria.
- La “revisión de la auditoría” extraordinaria.

En ambos casos, esta participación se deberá llevar a cabo en términos idénticos a los de las fases anteriores, y la selección inicial de las empresas llevada a cabo anteriormente implicará irrenunciablemente, si fuese necesaria, la participación en esta fase.

3.2 LOTE 2 – Auditoría interna

La empresa adjudicataria de este lote deberá ofrecer, bajo el modelo de funcionamiento comúnmente conocido como “cesión de auditores”, las capacidades necesarias para que el Órgano de Auditoría Técnica de Cyberzaintza pueda llevar a cabo, a través de dichos servicios, las funciones de auditoría interna del OAT.

Para ello, el modelo de funcionamiento se estructurará de acuerdo con las fases descritas a continuación.

3.2.1 Fase preliminar: Establecimiento del programa de auditoría

Durante la fase previa a la prestación del servicio por parte de la empresa adjudicataria, el Organismo de Auditoría Técnica de la Agencia planteará un programa inicial de auditoría interna, en el que determine de manera preliminar:

- El número de auditorías internas a desarrollar a lo largo del año
- El alcance de cada una de dichas auditorías internas
- Los criterios de auditoría a utilizar, que serán, de manera general:
    - La norma ISO 17065
    - La guía CCN-STIC 122 - Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS
    - La CCN-STIC IC-01/19 - ENS. Criterios Generales de Auditoría y Certificación
    - La documentación interna del OAT
- Las fechas de referencia planteadas para cada una de las auditorías internas
- Otros aspectos que puedan ser relevantes para la prestación del servicio:
    - Modalidad de la auditoría (presencial / remota / mixta)
    - Idioma(s) de la auditoría
    - Etc.

Con esa información, la Agencia trasladará a la empresa adjudicataria la necesidad de activar los servicios de auditoría interna, con el fin de llevar a cabo la planificación de las auditorías internas.

3.2.2 Primera fase: Planificación de las auditorías internas

Con la empresa adjudicataria se concretarán, mediante el correspondiente diálogo entre todas las partes, para cada una de las auditorías internas consideradas:

- Los miembros específicos del equipo de trabajo que desempeñarán la auditoría interna.
- El número de jornadas específicas que se llevarán a cabo de manera presencial, remota y asíncrona, según corresponda en cada caso.
- Los días específicos que se llevarán a cabo de forma presencial y remota, según corresponda en cada caso.
- El horario en el que se llevarán a cabo las sesiones, tanto presenciales como remotas, cuando corresponda.
- La planificación específica de cada una de las sesiones presenciales y/o remotas, incluyendo todas las consideraciones necesarias.

Así mismo, la empresa adjudicataria procederá a la designación de las personas que vayan a participar en la auditoría interna.

3.2.3 Segunda fase: Lanzamiento de la auditoría

En esta fase se llevarán a cabo las firmas, por parte de todo el personal designado por la empresa adjudicataria, de las cláusulas nominales de *confidencialidad* y *ausencia de conflictos de interés*.

La auditoría interna se organizará y articulará de acuerdo con los procedimientos que el OAT de Cyberzaintza tiene establecidos a tal efecto. Si fuese necesario llevar a cabo algún tipo de replanificación o ajuste, se llevaría a cabo durante esta fase. Finalmente, la empresa adjudicataria será la responsable de asegurar la entrega, en tiempo y forma, del correspondiente *Plan de Auditoría Interna*.

3.2.4 Tercera fase: Ejecución de la auditoría

La auditoría se desarrollará de acuerdo con los procedimientos que el OAT de Cyberzaintza tiene establecidos a tal efecto. Durante esta fase, la labor de la empresa adjudicataria será la de desarrollar las funciones de auditor interno.

La fase de ejecución de la auditoría contemplará, de acuerdo con dichos procedimientos:

- La propia ejecución de la auditoría interna
- La generación del informe de auditoría interna correspondiente
- La evaluación del PAC, si fuese necesario.
- La determinación de las oportunidades de mejora

En esta fase, la empresa adjudicataria será la responsable de asegurar la entrega, en tiempo y forma, del correspondiente *Informe de Auditoría Interna*, incluyendo expresamente las oportunidades de mejora que se hayan podido identificar.

3.2.5 Cuarta fase: Auditoría extraordinaria

En caso de que el proceso de auditoría interna requiera el desarrollo de una auditoría extraordinaria, la empresa adjudicataria deberá participar, desarrollando las mismas funciones que en la auditoría ordinaria, en:

- La “planificación de la auditoría” extraordinaria.
- El “lanzamiento de la auditoría” extraordinaria.
- La “ejecución de la auditoría” extraordinaria.

Dicha participación se deberá llevar a cabo en términos idénticos a los de las fases anteriores.

4 DEFINICIÓN DEL SERVICIO

4.1 Fases del servicio

Se identifican las siguientes fases:

4.1.1 Preparación del servicio

El periodo de preparación del servicio tendrá una duración máxima de cuatro semanas, y consiste en el tiempo necesario para su activación práctica. En este periodo se deberá determinar:

- Los mecanismos de interacción entre la Agencia y las empresas adjudicatarias.
- El personal específico que participará en la prestación de los servicios, junto con sus perfiles.
- Los mecanismos de gestión del servicio.

Por parte de Cyberzaintza, durante esta fase se proporcionará:

- Una programación preliminar de las posibles auditorías (de certificación e interna) que se podrían llevar a cabo durante el periodo de duración del servicio.
- Una formación inicial a todas las personas que van a participar en la prestación de los servicios acerca de los procedimientos del Órgano de Auditoría Técnica que deberán seguir.
- Las cláusulas iniciales específicas de pertenencia al OAT, que todos los afectados deberán firmar individualmente.

Una vez finalizada la fase de preparación, 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 preparación y finalizará con el inicio de la fase de devolución del servicio.

Desde el inicio del servicio, existirá una comunicación como mínimo mensual entre la Agencia y las empresas adjudicatarias del servicio con el fin de realizar actualizaciones periódicas del programa de auditorías previsto.

La selección de las empresas a participar en cada una de las auditorías se llevará a cabo una vez que la Agencia disponga de la confirmación, por parte del organismo público, de que efectivamente va a contar con Cyberzaintza para la realización de su auditoría de certificación de conformidad con el ENS.

Una vez seleccionadas las empresas que van a participar en cada una de las auditorías, tanto en su ejecución como en la revisión de su expediente, las citadas empresas deberán designar al personal específico que va a participar en la auditoría correspondiente, que deberá ser, en todo caso:

- Personal que cuente con la cualificación correspondiente, de acuerdo con lo establecido.
- Personal que haya participado en la formación inicial durante la fase de preparación del servicio.

Una vez designado el personal que va a desarrollar las funciones de auditor jefe, auditor, revisor de expedientes y/o auditor interno, dichas personas deberán funcionar de manera autónoma,

resolviendo adecuadamente y en los plazos marcados las tareas encomendadas, gestionando los recursos y obteniendo los resultados e informes establecidos.

Por parte de la Agencia se podrán especificar herramientas concretas en las que se desea se reporte parte o toda la información relativa a las actividades desarrolladas y/o los informes generados.

4.1.3 Devolución

Las empresas adjudicatarias estarán obligadas a prestar apoyo, y realizar la transferencia de conocimiento, documentación, etc. a las siguientes empresas adjudicatarias del contrato, en caso de que estas sean distintas a las empresas adjudicatarias del presente pliego.

El plazo máximo para la fase de devolución no será superior a cinco 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

Los entregables correspondientes en cada caso serán, al menos, los reflejados en el apartado correspondiente.

Puede ser necesario que los entregables del proyecto se entreguen en formato bilingüe, es decir, en euskera y castellano, respetando la calidad lingüística y técnica de ambos idiomas. En dicho caso, 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. El desarrollo bilingüe de los entregables no supondrá, en ningún caso, ningún tipo de sobrecoste para la Agencia.

A continuación, se incluyen algunos ejemplos de posibles entregables. En cualquier caso, los entregables aquí detallados se deben considerar como una primera aproximación. Las empresas adjudicatarias 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.

-
- **Lote 1 Auditorías de conformidad:**
  - Acuerdos de confidencialidad
  - Acuerdos de ausencia de conflicto de interés
  - Plan de Auditoría
  - Informe de Revisión de Actividades Previas a la Auditoría
  - Informe de Auditoría
  - Recomendación del Auditor Jefe al Comité de Certificación
  - Informe de Revisión del expediente.
  - Adopción de decisión de certificación.
  - Cualesquiera otros que las empresas adjudicatarias consideren necesarios.

- **Lote 2 Auditorías internas:**

- Acuerdos de confidencialidad
- Acuerdos de ausencia de conflicto de interés
- Plan de Auditoría
- Informe de Auditoría
- Cualesquiera otros que la empresa adjudicataria 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, las empresas o entidades adjudicatarias deberán 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, se hace necesario que el equipo realice la actividad en los siguientes términos:

- Podrá ser necesario llevar a cabo reuniones de seguimiento del servicio de manera presencial en las oficinas de Cyberzaintza, a las que será imprescindible la asistencia de una figura Responsable del servicio.
- En función de las necesidades del servicio podrá ser necesaria la presencia del equipo de trabajo en las ubicaciones y dependencias tanto de la Agencia como de los organismos públicos destinatarios de las auditorías (cuyo alcance geográfico podrá ser cualquier localidad del País Vasco) para la recogida de datos, sesiones de trabajo u otro tipo de reuniones.

Los medios de tratamiento de toda la información y documentación a la que se tenga acceso durante las auditorías (correo electrónico, sharepoint, AMPARO, etc.) serán los de 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.

4.4 Equipo de trabajo

Para cada uno de los lotes será necesario contar con los siguientes roles:

- Responsable del servicio.
- Auditores (con capacidad para desempeñar las funciones de auditor jefe, auditor, responsable de expedientes y/o auditor interno).

4.4.1 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.

4.4.2 Auditores

Las personas con rol de Auditores (independientemente de que desarrollen funciones de auditor jefe, auditor o revisor de expedientes) tendrán la capacitación necesaria para ejercer la función de auditor jefe, y acreditarán la experiencia necesaria en la realización de tareas similares a las descritas para el lote correspondiente. Se responsabilizarán de las actividades del servicio de manera íntegra, dentro de la función que desempeñen en cada momento.

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

- Que en la propia empresa cuenten formalmente con la cualificación oficial como auditores jefe.
- Que cuenten con formación en auditorías de sistemas de información, a través de certificaciones reconocidas a nivel nacional o internacional, cursos, seminarios o actividades formativas regladas o impartidas por entidades reconocidas, de calidad y adecuado número de horas formativas que permitan evidenciar la idoneidad y suficiencia de los conocimientos adquiridos.
- Que dispongan de experiencia verificable en la realización regular de auditorías o inspecciones de tecnologías de la información de, al menos, 20 jornadas en los últimos 4 (cuatro) años, de las cuales, 10 tienen que haberse realizado en el último año.
- Que cuenten con conocimiento de seguridad y gestión de riesgos de seguridad, demostrable por medio de certificaciones o experiencia de, al menos, 4 (cuatro) años en estas competencias.
- Que cuenten con conocimiento de los requisitos del RD 311/2022, demostrable por medio de cursos o seminarios sobre estas competencias, de calidad y alcance suficientes, que comprendan un mínimo de 20 horas de formación.
- Que dispongan de conocimientos de la legislación aplicable cuando la auditoría pueda requerir la evaluación de la conformidad de medidas derivadas del cumplimiento de otras normativas, tales como las de protección de datos, o el Esquema Nacional de Interoperabilidad, Identidad Electrónica, Firma Electrónica y Servicios de Confianza, entre otras.
- Que estén familiarizados con las Guías de Seguridad CCN-STIC aplicables, y disponer de conocimientos en la administración de seguridad de sistemas operativos y aplicaciones, así como en infraestructuras de redes informáticas y mecanismos criptográficos.
- Que puedan evidenciar conocimiento de la norma ISO/IEC 17065.

Así mismo, será valorable, de acuerdo con lo establecido en el proceso de licitación, la capacidad de los auditores para llevar a cabo las funciones correspondientes de forma bilingüe, en euskera y castellano, con la correspondiente calidad lingüística y técnica en ambos idiomas, así como la experiencia específica de cada uno de ellos.

4.5 Dimensionamiento y dedicación

Las propuestas deben dimensionar los recursos necesarios para prestar el servicio, cumpliendo todos los requisitos, de acuerdo con lo establecido en el proceso de licitación. No obstante, se establecen los siguientes criterios mínimos:

- Para el Lote 1, relativo a las auditorías de certificación, se deberán designar en la propuesta, al menos, dos recursos nominales específicos capaces de llevar a cabo las funciones de auditor jefe, auditor o revisor de expedientes.
- Para el Lote 2, relativo a la auditoría interna, se deberá designar en la propuesta, al menos, un recurso nominal específico capaz de llevar a cabo las funciones de auditor interno.

5 EJECUCIÓN DEL CONTRATO

Las empresas adjudicatarias serán responsables del correcto desarrollo de los trabajos solicitados relacionados, de acuerdo con los requerimientos del presente pliego.

5.1 Supervisión del contrato

La actuación de las empresas adjudicatarias será supervisada por la persona responsable que la Agencia Vasca de Ciberseguridad designe. Asimismo, las empresas adjudicatarias designarán 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 la realización de reuniones de seguimiento, que se celebrarán mensualmente para revisar el grado de cumplimiento de las tareas planificadas, las programaciones de actividades a realizar, etc.

5.2 Horario del servicio

Para la ejecución de las tareas especificadas en este contrato, se requiere que las empresas adjudicatarias dispongan del personal necesario al menos durante la jornada laboral, independientemente de si los trabajos se realizan de forma presencial o mediante teletrabajo.

Asimismo, las empresas adjudicatarias deben 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.

5.3 Asignación del Personal

Los perfiles propuestos para prestación del servicio deben ser nominales, **no admitiéndose perfiles genéricos**. Las empresas licitadoras deberán aportar el detalle de las cualificaciones profesionales del equipo propuesto para la prestación del servicio. Con este propósito, deberán 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.

Las empresas licitadoras se comprometen, en caso de ser adjudicatarias, 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 de éste. En el caso de modificación o sustitución de recursos, deberán 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 asignados 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.

5.3.1 Constitución inicial del equipo de trabajo

El equipo técnico que incorporar tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por los recursos 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.

5.3.2 Modificaciones en la composición del equipo de trabajo

Si las empresas adjudicatarias propusieran 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.

No obstante, la designación de las personas que componen el Equipo de Trabajo realizada por las empresas adjudicatarias podrá ser modificada, a simple petición de la Agencia, y en este caso, las empresas adjudicatarias se obligan 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 las empresas adjudicatarias.

5.4 Registro y Control

Como parte del contrato, las empresas adjudicatarias estarán obligadas a dar total cumplimiento a las condiciones que al efecto de control establezca la Agencia.

Las empresas adjudicatarias deberán 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 los servicios a los pliegos de cláusulas administrativas, a este pliego de prescripciones técnicas y a las ofertas de las empresas adjudicatarias. En tal sentido las empresas adjudicatarias deberán 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 las empresas adjudicatarias 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

Las empresas contratistas deben 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 las empresas contratistas no podrán 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. Las empresas contratistas quedan obligadas a poner todos los medios a su alcance para preservar el secreto y confidencialidad de la información a la que tengan acceso durante la ejecución del contrato.

6.2 Ausencia de conflictos de interés

Las empresas adjudicatarias se comprometen a que, antes de participar en la auditoría que les pueda ser asignada, han comprobado que no están sujetas a ninguna asociación o vinculación previa o actual por su parte con los organismos públicos auditados ni con los sistemas de información auditados, en su caso. Este compromiso incluye la ausencia de conflictos de interés vinculados con relaciones personales, familiares, laborales, intereses financieros, pertenencia a organizaciones, consultorías o asesorías previas, factores organizativos, competencia, posibilidad de futuro negocio, u otros aspectos pertinentes.

En el ejercicio de sus funciones, las empresas adjudicatarias centrarán su actuación exclusivamente en la realización de los servicios requeridos, garantizando en todo momento la imparcialidad, independencia y rigor técnico.

En este sentido, se comprometen a:

- Mantenerse al margen de cualquier actividad de consultoría vinculada al proceso de implantación de medidas de seguridad, redacción de documentación o configuración y adaptación de sistemas.
- Abstenerse de emitir recomendaciones particulares sobre tecnologías, productos, herramientas o soluciones comerciales específicas que puedan influir en las decisiones técnicas del auditado.
- Respetar estrictamente los límites del rol que tiene asignado, sin asumir responsabilidades o tareas que correspondan a funciones operativas, de diseño o implementación dentro del sistema evaluado.

Así mismo, las empresas adjudicatarias se comprometen a comunicar, antes de la formalización del Equipo Auditor, sobre cualquier situación que pueda presentar un conflicto de interés o generar dudas razonables.

6.3 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.

Las empresas contratistas se verán también obligadas a guardar las normas vigentes sobre Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vean obligadas a manejar.

Al finalizar el contrato, una vez haya sido transferida la información a la Agencia Vasca De Ciberseguridad, las empresas contratistas se comprometen 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.