Osakidetza

ZUZENDARITZA NAGUSIA
DIRECCIÓN GENERAL

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Contratación de servicios de consultoría para el seguimiento normativo de la seguridad TIC en Osakidetza

2020/02423

Araba kalea, 45 – 01006 VITORIA-GASTEIZ
Tfnoa. 945006000
www.**Osakidetza**.euskadi.eus

EUSKO JAURLARITZA
GOBIERNO VASCO
OSASUN SAILA
DEPARTAMENTO DE SALUD

0. INDICE

Página

0. INDICE 2
1. OBJETO DEL CONTRATO 4
2. AMBITO Y ALCANCE DEL CONTRATO 4
2.1. Organizaciones implicadas o lugar de prestación y/o ejecución 4
2.2. Alcance del contrato 4
2.2.1. Plan de adecuación y certificación en el esquema nacional de seguridad 4
2.2.1.1. Elaboración del Plan de Adecuación y Certificación en el Esquema Nacional de Seguridad 4
2.2.1.2. Ejecución del Plan de Implantación del Esquema Nacional de Seguridad aprobado 5
2.2.2. Servicio de consultoría para el desarrollo e implantación de un sistema de gestión de continuidad de negocio 5
2.2.3. Implantación de un sistema de información corporativo que dé soporte al Esquema Nacional de Seguridad y al Sistema de Gestión de la Continuidad del Negocio. 6
2.2.4. Servicio de consultoría para elaborar un plan de adecuación a la norma ISO 27001 (Sistema de Gestión de Seguridad de la Información). 6
3. LOTES 7
4. REQUISITOS NORMATIVOS GENERALES Y ETIQUETAS 7
5. REQUISITOS TÉCNICOS GENERALES 7
6. VARIANTES TECNICAS 7
7. MUESTRAS 7
8. PLAN DE TRABAJO / PROGRAMA DE TRABAJO /PLAN DE PUESTA EN MARCHA / LUGAR DE ENTREGA SUMINISTRO 7
8.1. Plan de Trabajo 7
8.2. Fases del servicio 8
8.2.1. Fase de análisis de la situación actual 8
8.2.2. Fase de ejecución del servicio 8
8.2.3. Fase de finalización del servicio 8
8.3. Entregables 8
8.4. Cronogramas 9
8.5. Ubicaciones 9
9. MODELO DE GESTIÓN DE SERVICIO 10

9.1. Equipo organizativo _____ 10
9.2. Modelo de control y seguimiento _____ 10
10. EJECUCION _____ 12
10.1. Condiciones de ejecución _____ 12
10.1.1. Horario _____ 12
10.1.2. Condiciones especiales de ejecución _____ 12

1. OBJETO DEL CONTRATO

En cumplimiento con las exigencias normativas en materia de seguridad TIC, **Osakidetza** requiere contratar servicios de consultoría con el fin de dar apoyo al plan de mejora continua en su política en materia de protección de la información. Siendo las áreas de trabajo objeto del presente concurso el Esquema Nacional de Seguridad y la Continuidad de Negocio.

Se establecen como objetivos finales de la consultoría solicitada la certificación en el Esquema Nacional de Seguridad y el desarrollo de un Sistema de Gestión de la Continuidad del Negocio en el área de Tecnologías de Información (TIC) de **Osakidetza**.

2. AMBITO Y ALCANCE DEL CONTRATO

2.1. Organizaciones implicadas o lugar de prestación y/o ejecución

Los servicios solicitados se prestarán a la red **Osakidetza**.

2.2. Alcance del contrato

Los servicios objeto del presente contrato se detallan a continuación.

- Servicios de consultoría para la elaboración y seguimiento del 'Plan de adecuación y certificación en el esquema nacional de seguridad'
- Servicio de consultoría para el desarrollo e implantación de un sistema de gestión de continuidad de negocio.
- Servicio de implantación de un sistema de información corporativo que dé soporte al Esquema Nacional de Seguridad y al Sistema de Gestión de la Continuidad del Negocio.
- Servicio de consultoría para elaborar un plan de adecuación a la norma ISO 27001 (Sistema de Gestión de Seguridad de la Información).

2.2.1. Plan de adecuación y certificación en el esquema nacional de seguridad

Siendo el detalle de los servicios solicitados:

2.2.1.1. Elaboración del Plan de Adecuación y Certificación en el

Esquema Nacional de Seguridad

El licitador deberá elaborar la propuesta de Plan de Adecuación y Certificación en el Esquema Nacional de Seguridad para su validación y aprobación por parte de **Osakidetza**. Dicho plan debe recoger un plan de trabajo detallado que recoja las necesidades actuales de **Osakidetza** y que facilite su consecución en el plazo establecido.

A partir de dicha propuesta el licitador deberá proporcionar los servicios de soporte y seguimiento necesarios para lograr la validación y aprobación formal del Plan de Adecuación y Certificación en el Esquema Nacional de Seguridad de Osakidetza, con el fin de constituir el hito requerido.

2.2.1.2. Ejecución del Plan de Implantación del Esquema Nacional de Seguridad aprobado

El licitador deberá proporcionar los servicios de soporte y seguimiento necesarios para lograr la correcta ejecución del Plan de Adecuación y Certificación en el Esquema Nacional de Seguridad de Osakidetza, en los plazos establecidos.

Debiendo contemplar la implantación de todas las medidas de seguridad consideradas, relativas tanto al despliegue y afianzamiento de los cambios organizativos, operativos y/o técnicos planteados como a la ejecución de las actividades relacionadas con el seguimiento y revisión de los resultados obtenidos como son:

- Formalización, consolidación y difusión de las medidas de seguridad implantadas, incluyendo píldoras periódicas de formación en el ámbito de la Seguridad al personal implicado.
- Desarrollo del proceso de gestión de la seguridad y puesta en marcha del proceso de mejora continua, integrando la seguridad en el ciclo de vida de los servicios y sistemas.
- Ejecución de la auditoría de seguridad y elaboración de la declaración de conformidad con el Esquema Nacional de Seguridad requerida.
- Revisión de las medidas adoptadas siguiendo una metodología PDCA.

2.2.2. Servicio de consultoría para el desarrollo e implantación de un sistema de gestión de continuidad de negocio

El licitador deberá proporcionar los servicios necesarios para el desarrollo e implantación de un sistema de continuidad de negocio en **Osakidetza**.

El desarrollo e implantación del Sistema de Gestión de la Continuidad del Negocio deberá comprender al menos, los siguientes aspectos:

- Desplegar la estructura organizativa y funcional necesaria para garantizar la implantación, desarrollo, seguimiento y mejora del Sistema de Gestión de la Continuidad del Negocio.
- Desarrollar un Análisis de Impacto en el Negocio o BIA (Business Impact Analysis) que permita identificar las necesidades y expectativas de la organización en materia de continuidad.
- Identificar los servicios disruptivos para el negocio e integración en el Plan de Continuidad, recogiendo los ámbitos críticos para el negocio y estableciéndolos como base del Plan de Continuidad del Negocio para su vinculación con los servicios electrónicos, aplicaciones e infraestructuras (internas o externas).
- Definir el Plan de Continuidad y los Planes de Recuperación que permitan gestionar apropiadamente tanto la prevención frente a incidentes como la reacción en caso de que se lleguen a producir.
- Desarrollar un programa de pruebas que garantice la capacidad de la organización para responder ante incidentes que puedan poner en riesgo su continuidad.
- Implantar un programa de gestión de la continuidad del negocio, desarrollando todas aquellas actividades que garanticen la mejora continua y la adopción de una metodología PDCA en relación al Sistema de Gestión de la Continuidad del Negocio.
- Lograr en última instancia un Sistema de Gestión de la Continuidad del Negocio sencillo, eficaz y eficiente.

2.2.3. Implantación de un sistema de información corporativo que dé soporte al Esquema Nacional de Seguridad y al Sistema de Gestión de la Continuidad del Negocio.

El licitador proporcionará a **Osakidetza** una herramienta de software que de soporte a los servicios solicitados. Siendo alcance del presente contrato:

- Licencia corporativa
- Implantación de la solución
- Mantenimiento del sistema de información

2.2.4. Servicio de consultoría para elaborar un plan de adecuación a la norma ISO 27001 (Sistema de Gestión de Seguridad de la Información).

El licitador deberá elaborar un plan de adecuación a la norma ISO 27001 de Sistema de Gestión de Seguridad de la Información, para alinear los procesos, metodologías y prácticas de seguridad de la organización con los principios y requisitos de la norma ISO 27001.

3. LOTES

No

4. REQUISITOS NORMATIVOS GENERALES Y ETIQUETAS

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

5. REQUISITOS TÉCNICOS GENERALES

El licitador deberá incluir y asumir en su oferta económica el software o herramientas que formen parte del proyecto.

6. VARIANTES TECNICAS

No.

7. MUESTRAS

No.

8. PLAN DE TRABAJO / PROGRAMA DE TRABAJO /PLAN DE PUESTA EN MARCHA / LUGAR DE ENTREGA SUMINISTRO

8.1. Plan de Trabajo

Se deberá describir el plan de trabajo detallado para desarrollar los servicios solicitados, en el plazo de tiempo establecido y con la garantía de calidad requerida. Este plan de trabajo deberá detallar las actividades y tareas a realizar, identificando cuáles serán de su competencia y cuales corresponden a **Osakidetza**.

Se deben estimar todos los esfuerzos asociados a su ejecución, tanto por parte del licitador como por parte de **Osakidetza**, y se debe proponer una planificación temporal.

El ámbito de aplicación del presente contrato debe alcanzar todos los servicios prestados

por **Osakidetza** a cualquiera de los colectivos (ciudadano, empleado y empresas), y comprender todas las infraestructuras tecnológicas que los soportan.

8.2. Fases del servicio

La ejecución del servicio se ajustará a las siguientes fases:

8.2.1. Fase de análisis de la situación actual

En esta fase inicial se realizará un análisis de la situación actual respecto al cumplimiento de **Osakidetza** al Esquema Nacional de Seguridad.

La duración de esta fase no deberá ser superior a un mes.

8.2.2. Fase de ejecución del servicio

Esta fase se caracteriza por la prestación normal del Servicio según lo requerido en el presente pliego, tanto a nivel operativo (ejecución del servicio), como de gobierno (comités de seguimiento del servicio).

En el transcurso de la ejecución del contrato podrán surgir nuevas necesidades, pero siempre dentro del ámbito general del servicio y de los perfiles adscritos al servicio

8.2.3. Fase de finalización del servicio

La fase de finalización del servicio transcurrirá durante las semanas previas a la finalización del contrato, en las que se revisará toda la documentación que se haya redactado en el transcurso de la ejecución de este servicio.

8.3. Entregables

Por cada uno de los servicios solicitados, el licitador deberá detallar el conjunto mínimo de entregables a proporcionar junto con una descripción de su contenido.

En cualquier caso, el adjudicatario deberá proporcionar aquellos entregables mínimos necesarios para garantizar el adecuado cumplimiento de las exigencias del Esquema Nacional de Seguridad como son:

- Organización de la seguridad
- Normativas de seguridad
- Procedimientos de seguridad
- Proceso de seguridad
- Informe de auditoría

- Informe de cumplimiento

Y respecto al Sistema de Gestión de la Continuidad del Negocio:

- Análisis de Impacto en el Negocio
- Plan de Continuidad
- Planes de recuperación
- Plan de pruebas

Así mismo, el proveedor del servicio deberá proporcionar todos los entregables necesarios para llevar a cabo la adecuada gestión y seguimiento de los servicios solicitados, incluyendo al menos:

- Planificación detallada
- Actas de seguimiento
- Informes periódicos
- Informe ejecutivo

Los entregables aquí detallados se deben considerar como una primera aproximación, ya que por cada hito se acordará en los órganos de gobierno cada uno de los entregables a generar, así como el "contenido" detallado de cada uno de ellos, convenidos con el objetivo de asegurar la calidad final del proyecto realizado.

8.4. Cronogramas

El licitador deberá presentar en Diagramas de Gantt o Cronogramas de las Fases y Tareas propuestas para la ejecución de las realizaciones objeto del presente pliego.

8.5. Ubicaciones

El servicio se prestará desde la ubicación que el licitador tenga establecida para este tipo de servicios.

Es imprescindible que cuando el servicio se proporcione desde las instalaciones del adjudicatario, se cumplan las medidas especificadas sobre seguridad física y de accesos establecidas por **Osakidetza** para este tipo de servicios.

Osakidetza podrá solicitar de forma puntual o permanente, que el servicio (parte o todo) se preste desde una de sus ubicaciones. Caso de darse un cambio de ubicación, el coste asociado no debe repercutirse a **Osakidetza**.

9. MODELO DE GESTIÓN DE SERVICIO

9.1. Equipo organizativo

Las empresas interesadas presentarán en su propuesta la descripción de su equipo de trabajo, especificando los recursos humanos que destinarán al proyecto, sus perfiles profesionales, y las dedicaciones por cada una de sus categorías.

Existirá un Responsable del Servicio por parte de la empresa adjudicataria, representante de la misma e interlocutor y responsable de los trabajos ante la Dirección de **Osakidetza**.

Osakidetza aportará también la figura de un Responsable del Servicio, con la función de coordinar la participación de los recursos humanos corporativos, que sean necesarios en cada momento.

Osakidetza controlará, mediante la figura de su Responsable de Servicio, el cumplimiento de los términos acordados, así como la calidad y adecuación del objeto de este contrato, quedando ambos sujetos a lo que marca la Ley de Contratos de las Administraciones Públicas (texto refundido), en cuanto hace referencia a completar los términos y calidad de los productos desarrollados.

Los recursos humanos, perfiles y conocimientos deberán dimensionarse de la manera más adecuada para dar respuesta a las necesidades del proyecto:

- **Responsable del Proyecto**, con conocimiento en la Dirección y Coordinación de Proyectos en el marco de las Administraciones Públicas en el sector sanitario. Se exigirá la certificación '***Certificación Lead Auditor ISO 27001'.*** El Director del Proyecto será el responsable de la coordinación y dirección de las tareas del equipo de trabajo y el interlocutor ante el Director del Proyecto por parte de **Osakidetza**. La dedicación mínima será del 10% del total del servicio.

- **Consultor especialista** con conocimientos en las siguientes áreas: Esquema Nacional de Seguridad, Continuidad de Negocio y Protección de Infraestructuras Críticas, así como en las herramientas de gestión TIC de Osakidetza (Service Manager). Se exigirá las certificaciones: ***Certificación Lead Auditor ISO 27001***, ***Certificación Lead Auditor ISO 22301, Director de Seguridad, preferiblemente especialista en Infraestructuras Críticas y Estratégicas.***

La empresa licitante deberá entregar una tabla resumen, en la que se recoja la relación nominal de los componentes del equipo de trabajo ordenada por perfil ofertado y su dedicación al proyecto.

9.2. Modelo de control y seguimiento

Durante el desarrollo y ejecución, **Osakidetza** podrá establecer controles de calidad sobre la actividad desarrollada.

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.

El licitador describirá en su propuesta un Modelo de Gobierno, así como los mecanismos de reporte y compartición de información que considere oportuno.

Mínimamente deberá establecer los siguientes comités:

El **Comité de Dirección del Servicio:** Con carácter general se reunirá trimestralmente y será el foro donde se tratarán aspectos críticos que puedan afectar a la calidad y ejecución de los servicios solicitados.

El **Comité de Seguimiento:** Con carácter general se reunirá una vez al mes y será el foro donde se analizará y concretará:

- El grado de cumplimiento de las tareas planificadas
- Las programaciones de las actividades a realizar
- Informes de situación y progreso, con los que la empresa adjudicataria comunicará a la Dirección del Servicio de **Osakidetza**, del estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc.
- Hojas de control de tareas
- Documentos de gestión de proyectos: la empresa adjudicataria cumplimentará los documentos de gestión de proyectos, según un modelo definido (actas de reuniones, informes de progreso, etc.) verificando **Osakidetza** su cumplimiento.
- Entregables: mensualmente se entregarán los productos obtenidos (documentación, código, etc.) obtenidos con independencia de su calificación de “definitivos” o no.

La periodicidad con la que se reunirán estos foros podrá variar en función de las necesidades de **Osakidetza** y podrán ser presenciales o virtuales.

10. EJECUCION

10.1. Condiciones de ejecución

Dado que Osakidetza se encuentra inmersa en el proceso de convergencia con EJIE en los ámbitos de Infraestructuras CPD, Comunicaciones, Seguridad, Puesto de trabajo y servicios corporativos unificados, será necesaria la coordinación con EJIE para la correcta ejecución de los trabajos solicitados.

10.1.1. Horario

Con carácter general, para los trabajos desarrollados en las dependencias del adjudicatario la jornada de trabajo estará distribuida de acuerdo a la establecida por el adjudicatario.

Para los trabajos que se desarrollen en las dependencias de **Osakidetza**, la jornada de trabajo se adecuará a la establecida por **Osakidetza** en cada momento del año.

10.1.2. Condiciones especiales de ejecución

La empresa adjudicataria declarará que durante la ejecución del contrato se aplicarán medidas que respeten el medioambiente a través del uso de tecnologías y equipamientos que favorezcan el ahorro energético, el consumo responsable y la promoción del reciclado de materiales.

Documento firmado por: CARMEN
RECALDE LANGARICA
En la fecha 16.12.2020 13:20:24 CET