Pliego de prescripciones técnicas particulares.

Título: servicio de apoyo a Izenpe para el mantenimiento y la mejora en la gestión de su sistema de seguridad de la información.

Número de expediente: IZNP_S_002_2026

Tipo: ☒ Servicios, Suministro, ☐ Mixto

CPV: 79417000-0

Izenpe 2026

Este documento es propiedad de Izenpe. Únicamente puede ser reproducido en su totalidad.

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus

Tabla de contenido

1.	Objeto y alcance	3
1.1.	Objeto Principal	3
1.2.	Componentes del Servicio	4
2.	Descripción detallada del servicio de consultoría	4
2.1.	Gestión estratégica y de gobernanza	4
2.2.	Gestión de riesgos y cumplimiento	5
2.3.	Gestión operativa de la seguridad	6
2.4.	Mejora continua y Auditoria	7
3.	Modelo de prestación del servicio	7
3.1.	Organización y perfiles del equipo	7
3.2.	Horario y dedicación	8
3.3.	Modelo de relación y supervisión	8
3.4.	Procedimiento de sustitución de personal	9
4.	Entregables y documentación	9
4.1.	Requisitos de la documentación	9
4.2.	Lista de entregables mínimos	9

1. Objeto y alcance

1.1. Objeto Principal

Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, Izenpe) tiene la consideración de *prestador de servicios de confianza* según lo determinado en el REGLAMENTO *(UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE y Reglamento 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento nº 910/2014*

El cumplimiento de dicho Reglamento, la naturaleza de los servicios de Izenpe, así como la naturaleza de las entidades de las que es medio propio exige la adecuación de los procedimientos y actividad de Izenpe a diferentes estándares y normativas, entre los que podemos destacar:

- ISO 27001:2022
- ISO 27701:2019
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (NIS2).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.
- Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.
- Estándares ETSI, definidos en el reglamento y en los actos de ejecución que lo desarrollan, entre los que destacamos:
    - ETSI EN 319 401 General Policy Requirements for TSPs
    - ETSI EN 319 411-1 Policy and security requirements for TSPs issuing certificates: Part 1 General requirements
    - ETSI EN 319 411-2 Policy and security requirements for TSPs issuing certificates; Part 2 Requirements for issuing EU qualified certified certificates
    - ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
    - ETSI TS 119 461 Policy and security requirements for trust service components providing identity proofing of trust service subjects

- ETSI TS 119 431-1 Policy and security requirements for Trust Service Providers; Part 1: TSP services operating a remote QSCD/SCDev
- ETSI TS 119 471 Policy and security requirements for Providers of Electronic Attestation of Attributes Services

Para garantizar el correcto cumplimiento de estas normativas, Izenpe precisa contar con un servicio de consultoría de apoyo, y una licencia de hasta 10 usuarios de la herramienta GlobalSuite Solution que facilite la documentación y control de las tareas implicadas.

El objetivo fundamental del servicio son labores de apoyo en consultoría que permitirán a Izenpe mantener las certificaciones ISO, ENS y ETSI actuales, así como las adecuaciones necesarias para la obtención de nuevas certificaciones que Izenpe determine oportunas durante la vigencia del presente servicio.

1.2. Componentes del Servicio

1. Suministro de Licencia de Software de GlobalSUITE Solution para 10 usuarios, al menos en los siguientes paquetes: Information Security, Risk Management, ENS, Compliance.

   La empresa adjudicataria se encargará de gestionar la renovación de la licencia, así como del soporte de primer nivel de la misma

2. Servicio de consultoría de apoyo: Labores de consultoría para el mantenimiento y la mejora del cumplimiento normativo en seguridad y privacidad

2. Descripción detallada del servicio de consultoría

2.1. Gestión estratégica y de gobernanza

Agrupa las diferentes actividades necesarias para asegurar la ejecución de las labores encomendadas, adoptando sus estándares, con los niveles de calidad requeridos y ayudando a su consolidación y evolución. La gestión del servicio incluye:

- La persona coordinadora/responsable del servicio asumirá la comunicación directa con Izenpe e informará de manera periódica sobre la evolución del servicio solicitado.
- Interlocución con la Dirección de Izenpe y con los responsables de cada área.
- Coordinar todos los recursos técnicos y humanos que deba proveer el adjudicatario para el cumplimiento de las exigencias del pliego.
- Asegurar la calidad en todas las entregas realizadas a la Dirección y al Comité de Seguridad, tanto de documentación, informes, presentaciones o cualquier entregable relacionado con la prestación de los servicios objeto de esta licitación según los estándares de calidad definidos por Izenpe.
- Contribuir activamente a la mejora continua de los servicios.

- Garantizar la correcta adquisición del conocimiento funcional y técnico necesario para la adecuada prestación de los servicios a lo largo de la vida del contrato.
- Gestionar adecuadamente el conocimiento recibido y generado a lo largo de la ejecución del contrato, garantizando su documentación y traspaso a Izenpe de forma periódica.
- Colaboración en la gestión de los proyectos de seguridad a acometer, así como colaboración en el seguimiento de estos y evaluación de los entregables a los que den lugar.
- Gestionar las labores de secretaría técnica referidas al Comité de Seguridad.
- Documentación de los controles e hitos en el marco del sistema de gestión de la seguridad y privacidad establecido por Izenpe, en las herramientas que Izenpe determine.
- Coordinación y colaboración con los siguientes servicios externalizados:
  - Formación y concienciación anual en seguridad.
  - Formación técnica a desarrolladores.
  - Análisis de vulnerabilidades trimestral y test de penetración anual.
  - Test de ingeniería social.
  - Auditoría certificación de ISO 27001.
  - Auditoría certificación de ISO 27701.
  - Auditoría certificación de eIDAS/ETSI.
  - Auditoría certificación ENS
  - Oficina técnica PISE (Plan de Infraestructuras Sensibles de Euskadi)
  - Proveedores: coordinación para el establecimiento de medidas que garanticen la cadena de suministro con el nivel de seguridad establecido por Izenpe
  - Puestos de RA: coordinación con las diferentes entidades que suscriban un acuerdo con Izenpe para prestar labores de RA y para el establecimiento de medidas que garanticen el seguimiento del marco de actuación establecido por Izenpe.

2.2. Gestión de riesgos y cumplimiento

Los servicios demandados dentro de este apartado incluyen:

- Categorización de los sistemas y análisis de riesgos
  - Identificación de los sistemas y activos de Izenpe. Elaboración y mantenimiento de un inventario.

- Elaboración de propuestas de categorización de los sistemas acorde al Esquema Nacional de Seguridad y asesoramiento a los responsables de la Información y de los servicios.
- Análisis de riesgos de los sistemas. Este análisis de riesgos debe ser completo, de forma que permita validar el conjunto de medidas de seguridad implantado, detectar la necesidad de medidas adicionales y justificar el uso de medidas de protección alternativas.

- Mantenimiento de las declaraciones de aplicabilidad
  - Colaboración en la redacción de los documentos de Declaración de aplicabilidad de las medidas del ENS, de la ISO 27001 y de la ISO 27701, así como la colaboración para la elaboración de los planes de adecuación que resulten
- Soporte en el ciclo de vida de desarrollo seguro
  - Participación en el ciclo de vida de desarrollo de aplicaciones, validando los requisitos no funcionales de los mismos desde el punto de vista de clasificación de la información y el servicio con respecto al ENS y la legislación vinculada a los mismos en especial la legislación de protección de datos.
  - Revisar los aspectos de seguridad en el intercambio de información con entidades externas.

2.3. Gestión operativa de la seguridad

Gestión de incidentes y vulnerabilidades: este servicio incluye el análisis y respuesta a los incidentes de seguridad detectados. Los servicios demandados dentro de este apartado incluyen:

- Investigación y análisis continuo de las alertas de seguridad recogidas por las distintas fuentes, evaluando sus características y riesgos y determinando si se trata de un incidente de seguridad, realizando la investigación forense del impacto de este. Se crearán tiques en la herramienta de Ejie para la gestión de dichos incidentes.
- Realizar propuestas de respuesta y contención para los incidentes de seguridad.
- Coordinación y seguimiento de las acciones propuestas para la contención o neutralización de los ataques o resolución de vulnerabilidades hasta su completa implementación.
- Comprobación de la eficacia de las medidas implantadas.
- Participación en los comités de crisis que pudieran crearse para el tratamiento de incidentes de especial relevancia.
- Emisión de informes sobre el seguimiento de los incidentes de seguridad, proporcionando estadísticas sobre el tiempo de resolución de estos, impactos, etc...

- Alerta de las vulnerabilidades emergentes identificadas (ej.: ataques de día 0, ataques a gran escala, vulnerabilidades de los productos utilizados en Izenpe, etc.) que puedan afectar a la seguridad de los activos de Izenpe, desarrollando propuestas de actuación para minimizar el riesgo de los ataques.

Coordinación con proveedores de ciberseguridad

2.4. Mejora continua y Auditoria

Los servicios demandados dentro de este apartado incluyen:

- Gestión del plan de mejora continua
- Definición y seguimiento de objetivos e indicadores
- Acompañamiento y seguimiento de auditorías externas (ISO, ENS, ETSI,..)
- Revisión y soporto al plan de continuidad de negocio

3. Modelo de prestación del servicio

3.1. Organización y perfiles del equipo

Para desempeñar los servicios objeto del contrato, los licitadores deberán contar con un equipo de trabajo que garantice el nivel de especialización requerido, lo que supone una permanencia del conocimiento a lo largo de la duración del contrato, tanto de aquel traspasado inicialmente, como del adquirido durante la prestación de los servicios.

Durante la ejecución del contrato, Izenpe se reserva el derecho de verificación de que los perfiles profesionales propuestos finalmente por el adjudicatario se ajustan a los requisitos de este pliego y a la oferta del adjudicatario en caso de que incluya mejoras sobre los requisitos mínimos establecidos.

La inadecuación de la capacitación y conocimientos del personal adscrito a la ejecución del contrato a los requerimientos exigidos para llevar a cabo todas sus prestaciones de forma correcta podrá dar lugar a la solicitud por parte de Izenpe de sustituciones de personas concretas, y en último término, a la resolución del contrato.

Perfiles mínimos requeridos:

Gerente del servicio (responsable del contrato): Será el interlocutor principal con Izenpe. Se encargará de la planificación, el seguimiento de las actividades, la gestión del equipo y la presentación de informes a la Dirección

Consultor/Especialista en Cumplimiento y seguridad: Ejecución de las tareas técnicas descritas en el pliego, como el análisis de riesgos, la gestión de incidentes, el mantenimiento del cuerpo normativo, el soporte en auditorías y la documentación en las herramientas designadas

3.2. Horario y dedicación

Las labores de interlocución con Izenpe, tendrán que llevarse a cabo dentro del horario laboral de la persona de Izenpe con la que se requiere la interlocución.

La interlocución con los servicios externalizados deberá ser acordada entre las partes intervinientes.

En la actualidad, el servicio se presta por un equipo de tres personas con un volumen de 1325h anuales, el volumen de horas ofertado no podrá ser inferior a 1056h.

3.3. Modelo de relación y supervisión

El modelo de supervisión del servicio define las reglas y los roles en la relación de Izenpe con el adjudicatario para el desempeño del servicio con los niveles de calidad y eficiencia exigidos.

La Dirección de Izenpe podrá delegar sus funciones en una persona de Izenpe. Asimismo, podrá incorporar las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo. La dirección, supervisión y aprobación de los trabajos corresponden a la Dirección de Izenpe, siendo sus principales funciones en relación con el objeto del presente pliego las siguientes:

- Velar por el cumplimiento de los trabajos exigidos y ofertados.
- Establecer, los estándares, metodologías y criterios que asegurarán la calidad de los trabajos ejecutados.

El seguimiento y control del contrato se efectuará sobre las siguientes bases:

- En caso de que la empresa proponga la utilización de cualquier otro software adicional no incluido en el entorno tecnológico definido, el uso de este deberá ser aprobado por Izenpe.
- Las adaptaciones metodológicas propuestas por la empresa, en caso de ser aceptadas por Izenpe, deben incluir un plan de transferencia inicial del conocimiento necesario.
- Seguimiento continuo de la evolución del servicio entre la Dirección de Izenpe y el responsable del servicio.
- El responsable del servicio deberá proporcionar al Comité de Seguridad un panel de seguimiento que refleje los siguientes puntos, con periodicidad al menos trimestral:
  - Información de actividades pendientes, en ejecución y realizadas indicando su estado.
  - Información de incidencias detectadas por servicio, así como su estado y seguimiento.
  - Panel de seguimiento a corto, medio y largo plazo, para actividades de larga duración, recurrentes y proyectos.

- Reuniones de seguimiento de la Dirección de Izenpe y del coordinador y el equipo que se determine, al objeto de revisar el grado de cumplimiento de los objetivos y corregir las desviaciones detectadas.

3.4. Procedimiento de sustitución de personal

A lo largo de la ejecución del contrato puede surgir la necesidad de sustitución de cualquiera de los recursos del equipo. La sustitución debe notificarse por el responsable del servicio a Izenpe con al menos 15 días de antelación a la fecha de sustitución. El procedimiento de sustitución es el siguiente:

- Por lo general, si se fuera a producir la sustitución de un miembro del equipo de trabajo habrá un proceso de transición de 10 días laborables mínimo para asegurar el traspaso de conocimiento entre el recurso saliente y el entrante. Este proceso de transición no supondrá incremento de coste alguno para Izenpe.
- La incorporación o sustitución de miembros del equipo de trabajo se realizará manteniendo al menos los requisitos establecidos como mínimos para cada categoría profesional concreta, y manteniendo o mejorando la oferta realizada por el adjudicatario en caso de que contuviera mejoras sobre el mínimo establecido.
- Los adjudicatarios efectuarán una propuesta de sustitución que será estudiada por el responsable del contrato de la misma manera que se hizo para la constitución inicial del equipo de trabajo. En caso de que se rechace la propuesta por no cumplir los requisitos del Pliego o de la oferta, los adjudicatarios deberán realizar una nueva propuesta.

4. Entregables y documentación

4.1. Requisitos de la documentación

Todas y cada una de las tareas realizadas para la ejecución del servicio deberán ser correctamente documentadas y consolidadas en el entorno documental que Izenpe indique. Toda la documentación generada durante la ejecución del contrato será propiedad exclusiva de Izenpe sin que los adjudicatarios puedan conservarla, ni obtener copia de esta o facilitarla a terceros sin la expresa autorización de Izenpe, que la daría en su caso previa petición formal motivada de los adjudicatarios.

Se entregará a Izenpe toda la documentación producida y utilizada por la empresa adjudicataria. La documentación deberá seguir las plantillas y estándares definidos por Izenpe, si así lo hubiera establecido.

4.2. Lista de entregables mínimos

Entregables recurrentes:

- Panel de seguimiento para el comité de seguridad: cuadro de mando con los indicadores y el estado de actividades pendientes, en ejecución y finalizadas, con periodicidad al menos trimestral
- Actas del comité de seguridad
- Informe trimestral de actividad: resumen de actividades realizadas, estado de los proyectos, incidentes gestionados y progreso del plan de mejora

Entregables anuales o bajo demanda

- Análisis de riesgos (anual)
- Declaraciones de aplicabilidad actualizadas (anual)
- Plan de mejora continua de la seguridad
- Informes de gestión de incidentes relevantes (bajo demanda)

Responsable de Contrato: Dª Raquel Garay Ruiz de Azua

Directora General de Izenpe: Dª. Izaskun Urrestarazu Amondarian