CONTRATACIÓN P.A.N.A.P.

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE S.A.

# PLIEGO DE CONDICIONES TÉCNICAS RELATIVO A CONTRATACIÓN PARA *ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE S.A.* DEL SERVICIO DE ASISTENCIA PARA ADECUACIÓN A AUDITORÍAS DE SEGURIDAD

Tabla de contenido


| | | |
|---|---|---|
| 1. | OBJETO Y ALCANCE | 3 |
| 2. | DESCRIPCIÓN GENERAL DEL SERVICIO | 4 |
| 2.1. | Gestión del servicio | 4 |
| 2.2. | Coordinación con proveedores | 4 |
| 2.3. | Gestión de incidentes de seguridad y vulnerabilidades | 5 |
| 2.4. | Categorización de los sistemas y análisis de riesgos | 5 |
| 2.5. | Mantenimiento y mejora continua del SGSI-SGPI | 6 |
| 3. | Modelo de relación y supervisión | 6 |
| 4. | Documentación | 7 |
| 5. | Horario de prestación del servicio | 8 |
| 6. | Organización de los adjudicatarios | 8 |
| 6.1. | Procedimiento de sustitución de recursos del equipo | 8 |

## 1. OBJETO Y ALCANCE

*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 (en adelante eIDAS).*

El cumplimiento de dicho Reglamento implica la necesidad de cumplir además con las siguientes normas:

- ISO 27001:2014
- ETSI EN 319 401 General Policy Requirements por 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
- EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- UNE EN 419 241-1 Trustworthy Systems Supporting Server Signing; Part 1 General Requirements
- 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

Además, con el objetivo de garantizar el cumplimiento del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD), Izenpe precisa de la certificación ISO 27701:2019 de gestión de información de privacidad.

Para garantizar el correcto cumplimiento de esta normativa y legislación, Izenpe precisa del servicio de asistencia técnica.

Los objetivos a cubrir en el servicio los determinará IZENPE, aunque irán orientados fundamentalmente al mantenimiento y evolución de las tareas implícitas en las diferentes normas ISO y ETSI en las que IZENPE está certificado.

## 2. DESCRIPCIÓN GENERAL DEL SERVICIO

### 2.1. Gestión del servicio

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

- Asegurar el nivel de interlocución con la Dirección de Izenpe y con 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.
- Mantenimiento del repertorio de proyectos de seguridad a acometer, así como colaboración en el seguimiento de los mismos y evaluación de los entregables a los que den lugar.
- Gestionar las labores de secretaría técnica referidas al Comité de Seguridad.

### 2.2. Coordinación con proveedores

Será necesaria la coordinación con los siguientes servicios externalizados:

- Formación y concienciación anual en seguridad.
- Formación técnica a desarrolladores.
- Auditoría de puestos de identificación (RAs).
- Análisis de vulnerabilidades trimestral y test de penetración anual.
- Test de ingeniería social.
- Auditorías a proveedores.
- Auditoría certificación de ISO 27001.
- Auditoría certificación de ISO 27701.
- Auditoría certificación de eIDAS/ETSI.

- Auditoría certificación CABForum.

### 2.3. Gestión de incidentes de seguridad 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 del mismo. Se crearán tickets 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 activa 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 los mismos, 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.

### 2.4. Categorización de los sistemas y análisis de riesgos

Los servicios demandados dentro de este apartado incluyen:

- 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.
- 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 de protección de datos.
- Análisis de riesgos de los sistemas utilizando la herramienta PILAR u otra en caso de que Izenpe así lo determinara. 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.
- Preparar la Declaración de aplicabilidad de las medidas del Anexo II del ENS, de la ISO 27001 y de la ISO 27701.

- Controlar aspectos de seguridad en el intercambio de información con entidades externas.

### 2.5. Mantenimiento y mejora continua del SGSI-SGPI

Los servicios que deberán prestarse dentro de este apartado incluyen, como mínimo:

- Revisión y mantenimiento del cuerpo normativo de seguridad de la información de Izenpe acorde a la Política de Seguridad de la Información, que se encuentra actualmente en proceso de revisión.
- Implementación del plan de mejora continua de la seguridad en Izenpe. Definición de objetivos e indicadores, y realización práctica de los mismos.
- Gestión y seguimiento de las siguientes auditorías requeridas:
  - 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
  - EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
  - ISO 27001:2014 Gestión de Seguridad de la Información
  - ISO 27701:2019 Gestión de Información de Privacidad
- Apoyo para la acreditación de cumplimento del Esquema Nacional de Seguridad siguiendo la guía CCN-STIC-809.
- Revisión del plan de continuidad de negocio y recuperación ante desastres. Se llevará a cabo un plan de continuidad de los servicios y de la infraestructura de soporte a los sistemas de información y telecomunicaciones ante posibles contingencias.
- Control de la calidad de la documentación, asegurándose que se ajusta a los estándares de Izenpe (formato, almacenamiento, control de versiones, histórico, etc.).
- Colaboración en la implantación de las medidas recogidas en el Reglamento General de Protección de Datos (RGPD).
- Elaboración de informes bajo petición, incluidos, aunque no limitados a: informe de estado de seguridad, informe de progresos de cumplimiento normativo, así como informes de control y seguimiento de los proyectos a su cargo.

## 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, 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.

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. 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 del mismo 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.

## 4. Documentación

Todas y cada una de las tareas realizadas para la ejecución del servicio deberán ser correctamente documentadas y consolidadas en el entorno documental de Izenpe (Atlassian). Toda la documentación generada durante la ejecución del contrato será propiedad exclusiva de Izenpe sin que los adjudicatarios puedan conservarla, ni obtener copia de la misma 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.

## 5. Horario de prestación del servicio

El horario laboral, a efectos de la ejecución del servicio, **será de 5 horas** y estará comprendido entre las 7:30 y las 15:00 de lunes a viernes durante todo el año.

## 6. Organización de los adjudicatarios

Para desempeñar los servicios objeto del contrato, los licitadores deberán contar con la capacidad productiva configurada en 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.

### 6.1. Procedimiento de sustitución de recursos del equipo

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.

| | |
|---|---|
| D. Oscar Garcia Jimeno<br><br>Responsable de Contrato<br><br>OSCAR GARCIA JIMENO<br>Firmado digitalmente por OSCAR GARCIA JIMENO<br>Fecha: 2021.06.25 08:53:34 +02'00' | Dª. Izaskun Urrestarazu Amondarian<br><br>15990846G MARIA IZASKUN URRESTARAZU (R: A01337260)<br>Firmado digitalmente por 15990846G MARIA IZASKUN URRESTARAZU (R: A01337260)<br>Fecha: 2021.06.25 09:08:52 +02'00'<br><br>*Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* |