PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR EN EL CONTRATO DE SERVICIOS PARA LA ASISTENCIA TÉCNICA Y SEGUIMIENTO DE MEDIDAS DE CONTROL PARA LA INFORMACIÓN,

EXPEDIENTE: E3/2022/05

1 CONTEXTO DEL CONSORCIO AUTORIDAD TERRITORIAL DEL TRANSPORTE DE GIPUZKOA. 3

2 OBJETO 4

3 ALCANCE Y ACTIVIDADADES DEL CONTRATO 5

3.1 Comité de seguridad 5

3.2 Cumplimiento de legislación vigente 5

3.3 Plan Director de seguridad de la información 6

3.4 Plan de continuidad de negocio 6

3.5 Eventos e incidentes de seguridad 7

4 EQUIPO DE TRABAJO 8

4.1 Requerimientos, acreditaciones 8

5 LA OFERTA DEBE INCLUIR: 9

1 CONTEXTO DEL CONSORCIO AUTORIDAD TERRITORIAL DEL TRANSPORTE DE GIPUZKOA.

El Consorcio Autoridad Territorial del Transporte de Gipuzkoa, en adelante ATTG, tiene como objetivo integrar todo el territorio de Gipuzkoa mediante un sistema de transporte sostenible.

La ATTG está formada por el gobierno Vasco, diputación foral de Gipuzkoa y Ayuntamientos de Donostia, Irun, Errenteria, Eibar, Zarautz, Arrasate, Hernani y Lasarte.

La ATTG lideró el proyecto de Integración Tarifaria de Gipuzkoa, Sistema MUGI, implantado con éxito en Gipuzkoa a partir del 4 de marzo de 2013.

El Sistema MUGI define una política tarifaria única en los servicios de autobuses urbanos de Gipuzkoa (Donostia, Irun, Errenteria, Eibar, Zarautz, Arrasate-Mondragón, Hernani, Lasarte-Oria, Oiartzun, Oñati y Tolosa), autobuses interurbanos (Lurraldebus 7 concesionarias), servicios ferroviarios de EuskoTren y Renfe, Todo ello mediante el uso de un único soporte de pago: la Tarjeta MUGI. Además, las tarjetas Mugi pueden ser también utilizadas posible en los tranvías de Vitoria y Bilbao, en el funicular de Larreineta, Tuvisa y Alavabus

En el sistema Mugi se encuentran activas más de 500.000 tarjetas (la gran mayoría personalizadas) y se realizan más de 60.000.000 viajes al año en transporte público. De ello se deriva que la ATTG gestiona un volumen muy elevado de datos tanto de carácter personal como de incidencia económica.

En consecuencia, la ATTG requiere de una asesoría experta en materia de seguridad haciendo especial hincapié en el RGPD y ENS

2 OBJETO

El alcance del servicio sería el siguiente:

- Apoyo al Comité de Seguridad de la Información.
- Asesoramiento en materia de cumplimiento de la legislación vigente en materia de seguridad de la información, destacando el Reglamento General de Protección de Datos, el Esquema Nacional de Seguridad y LOPDGDD
- Coordinación de la implantación de las medidas de seguridad recogidas en su plan director de seguridad de la información.
- Desarrollo de su plan de continuidad de negocio.
- Coordinación de la gestión y resolución de los eventos e incidentes en materia de seguridad de la información identificados en la operativa diaria de la ATTG.
- Asesoramiento en seguridad para la puesta en marcha de Mugi Virtual.

3 ALCANCE Y ACTIVIDADADES DEL CONTRATO

El alcance de esta propuesta de colaboración son todos los procesos y actividades de la ATTG y los activos que los soportan (hardware, software, comunicaciones, ubicaciones físicas, personas y proveedores).

Actividades y tareas a realizar:

3.1 Comité de seguridad

- Apoyo al Comité de Seguridad de la Información de la ATTG. Se dará apoyo al Comité de Seguridad de la Información de la ATTG. Este Comité tiene las siguientes funciones:
    - Definir, priorizar, coordinar y validar el cierre efectivo de las tareas pendientes en materia de seguridad de la información y continuidad de negocio de la ATTG.
    - Mejorar el desempeño del servicio que proporcionan los proveedores TI de la ATTG.

  En este Comité asiste al principal proveedor TI de la ATTG y se reúne como mínimo mensualmente. El servicio incluirá la elaboración del acta de reunión y relación de tareas pendientes. Puntualmente, se podrá requerir apoyo al otro Comité existente en la ATTG, de Atención a Personas Usuarias.

  Cara al seguimiento de tareas del comité de seguridad, la ATTG dispone de una herramienta basado en tickets para la gestión de incidencias. El adjudicatario deberá apoyar a la ATTG en su cumplimiento, seguimiento y control

3.2 Cumplimiento de legislación vigente

Se asesorará a la ATTG en el cumplimiento de la legislación vigente en materia de seguridad de la información, que sin ser ésta extensiva es principalmente:

- Reglamento (EU) 2016/679. Reglamento de la Unión Europea. Reglamento 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).
- Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero (modificado por el Real Decreto 951/2015, de 23 de octubre) (en adelante, ENS).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)

Adicionalmente, se atenderán todos los requerimientos:

Requerimientos informativos hacia los organismos de control (Agencia Vasca de Protección de Datos, Centro Criptológico Nacional, …). Dentro de estas tareas pueden enumerarse algunas como el apoyo en la cumplimentación de documentos y en los aplicativos EAR/PILAR, (Entorno de Análisis de Riesgos) INES (Informes de Estado de Seguridad en el ENS) del CCN-CERT y en los sea requerido para el cumplimiento del ENS.

También requerimientos y/o realización de tareas informativos hacia terceros (operadores, proveedores, Diputación Foral de Gipuzkoa, Gobierno Vasco).

3.3 Plan Director de seguridad de la información

Con toda la información generada en las actividades 3.1 y 3.2, el servicio implicará la implantación del plan director de seguridad de la información de la ATTG.

Dicho plan se estructura según el plan de adecuación ENS (nivel medio).

En apoyo a este plan Director la ATTG dispone de diversos documentos de seguridad tanto internos como necesarios a cumplir por los diversos proveedores que, por los servicios que prestan a la ATTG, así lo requieran.

El adjudicatario será el responsable de actualizar, adecuar, corregir los mismos o generar nuevos documentos cuando así se requiera

Sin ser exhaustivo, se pueden enumerar los siguientes:

- Política de seguridad de la información
- Normativa general de seguridad de la información
- Normativa general de seguridad de la información - Entidades proveedoras
- Control de la documentación
- Lista de control de documentos
- Lista de control de registros
- Autorización de uso
- Solicitud de autorización de uso
- Control de acceso
- Solicitud de alta, baja y modificación de acceso
- Registro de accesos
- Gestión de activos
- Gestión de las configuraciones
- Cambio en la configuración de los sistemas
- Revisión periódica de las especificaciones del equipamiento
- Programación de mantenimiento-revisión del equipamiento
- Registro de anomalías
- Gestión de cambios
- Gestión de incidencias
- Registro de incidencias
- Gestión de las copias de respaldo
- Planificación de las pruebas de recuperación
- Cláusulas - Propuesta general
- Cómo ejercer los derechos de acceso, rectificación, cancelación y oposición Acceso, rectificación, cancelación y oposición
- Clasificación de la información

El Plan director de Seguridad de información ni los documentos se entregarán a los licitadores en fase de licitación

3.4 Plan de continuidad de negocio

La ATTG dispone de un plan de continuidad de negocio. El servicio deberá:

- Mantener permanentemente actualizado el citado plan.
- Coordinar su aplicación ante caídas e intervenciones con parada en el servicio de la ATTG.
- Coordinar la planificación y realización de pruebas de al menos de un escenario por año.

Nota: Este plan de negocio no se pondrá en manos de los licitadores en fase de licitación

3.5 Eventos e incidentes de seguridad

La ATTG dispone de un procedimiento de registro y gestión de los eventos e incidentes de seguridad de la información que se detecten.

El servicio coordinará la resolución de todo lo detectado definiendo y apoyando la implantación de medidas correctivas para aquellos incidentes con impacto medio y alto.

- Apoyar a la ATTG en la elevación de consultas ante la AVPD.
- Redacción y en su caso revisión de informes que sean necesarios

4 EQUIPO DE TRABAJO

Las personas que trabajen en el servicio deben de disponer de al menos la siguiente experiencia demostrable mínima:

- 8 años en protección de datos de carácter personal.
- 6 años en el Esquema Nacional de Seguridad.
- 6 años en sistemas de gestión de seguridad de la información
- 6 años en sistemas de gestión-plan de continuidad de negocio

4.1 Requerimientos, acreditaciones

De Empresa:
serán necesarios acreditar los siguientes

- ISO20000,
- ISO27001, ISO22301,
- ENS MEDIO/ALTO

Individuales del equipo Consultor:

- Lead Auditor 20000,
- Lead Auditor 27001, Lead Auditor 22301,
- CISA
- ITIL V4 MANAGING PROFESSIONAL

El equipo de trabajo adscrito a este contrato deberá estar en posesión al menos de estas acreditaciones a la fecha de presentación de ofertas:

5 OFERTA

La oferta debe incluir como mínimo, los siguientes aspectos:

- Una memoria descriptiva de los puntos recogidos en los apartados 2 y 3 de este pliego h
    - Tendrán que realizar especial hincapié en lo señalado en los puntos 3.3 y 3.4. Respecto a estos apartados, deberán entregar una plan de trabajo y seguimiento de los mismos señalando los aspectos clave en cada uno de ellos.
- Metodología y planteamiento de las tareas a desarrollar.
- Las propuestas tendrán una extensión máxima de 35 páginas.