

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE SOFTWARE PARA LA GESTIÓN DE RIESGOS EMPRESARIALES Y DE CUMPLIMIENTO DE SERVICIOS DE TXINGUDI-TXINGUDIKO ZERBITZUAK, S.A.

**Código expediente:
24SUM003P1**

1.- OBJETO DEL CONTRATO

Suministro de software para la gestión de riesgos empresariales y de cumplimiento de SERVICIOS DE TXINGUDI-TXINGUDIKO ZERBITZUAK, S.A. (en lo sucesivo TXINZER), que permita la realización del proceso de identificación, análisis, evaluación y gestión de riesgos de manera distribuida y colaborativa entre los diferentes responsables de la entidad, así como el servicio de consultoría necesario para su correcto funcionamiento y uso.

El software deberá posibilitar la gestión integral de los riesgos a los que está expuesta TXINZER en el desarrollo de las actividades que constituyen su objeto social como operativos, legales, penales, económicos y reputacionales.

El software deberá posibilitar la gestión de los riesgos empresariales de acuerdo con lo Manual de Integridad de TXINZER, posibilitando la supervisión y control de la actividad empresarial por el Órgano de Cumplimiento e Integridad de la empresa, así como documentar todo el proceso llevado a cabo.

Código(s) CPV:

- 48900000-7 Paquetes de software y sistemas informáticos diversos
- 72000000-5 Servicios TI: consultoría, desarrollo de software, Internet y apoyo
- 71317000-3 Servicios de consultoría en protección y control de riesgos

2.- REQUISITOS TÉCNICOS

- La herramienta permitirá distribuirse en modalidad SaaS. La opción Cloud utilizará la infraestructura del fabricante de la solución y será el propio fabricante el encargado de su mantenimiento y actualizaciones de la solución.
- La herramienta será 100% web, es decir, los usuarios accederán a través de su navegador web.
- Todos los datos de la organización transmitidos a los servidores a través de redes públicas estarán protegidos mediante sólidos protocolos de encriptado.
- Todos los trabajos de implantación, actualización y mantenimiento deberán ser proporcionados por el oferente, durante la vigencia del contrato.
- SLA's de disponibilidad mayor a un 95% anual.

- Estará incluido el soporte 8*5, el cual incluirá el acceso al portal de soporte del fabricante donde la organización podrá realizar el seguimiento de sus casos y gestionarlos directamente con el fabricante.
- La herramienta deberá configurarse para el acceso a través de diferentes roles y perfiles de usuario.
- Permitirá la integración de forma nativa con el Directorio Activo de Txinzer a través de Azure Active Directory.
- Multiidioma: al menos español y euskera como idiomas obligatorios.
- Modulabilidad de áreas concretas hasta el total de la organización.
- SLA's del fabricante.

3.- REQUISITOS FUNCIONALES

- Las tareas definidas deberán poder llevarse a cabo a través de la plataforma implantada.
- Debe permitir el mantenimiento del sistema de gestión una vez realizadas las tareas de implantación.
- Debe permitir la certificación del sistema a través de la propia plataforma, centralizando toda la información requerida para la misma.
- Debe permitir la definición de la estructura organizativa (servicios, procesos, actividades, etc.)
- Debe permitir el inventariado técnico asociándolo a la estructura organizativa correspondiente.
- Debe permitir el ciclo completo de gestión de riesgos a través de la propia plataforma, incluyendo la configuración de diferentes metodologías, la gestión de controles y planes de acción.
- Permitirá modificar la configuración de las metodologías de análisis de riesgos y de controles a usuarios de la organización con permiso para ello y sin necesidad de la ayuda del oferente o fabricante de la solución.
- Debe incorporar un catálogo de riesgos y controles estandarizado en el que se puedan incorporar los catálogos de riesgos y controles utilizados por la organización.
- Permitirá la definición de amenazas en función de categorías como son Procesos, Información, Hardware, Software u otras identificadas por la organización facilitando la asignación de amenazas a cada categoría.
- Permite la definición y despliegue de encuestas para el levantamiento de información de datos personales, riesgos y controles de manera distribuida. Será posible acceder a las encuestas publicadas sin necesidad de entrar en la herramienta. También consolidar la información recibida.
- Permitirá la planificación centralizada de las auditorías, tanto internas como externas, que se realizan en el Sistema de Gestión.
- Permitirá descargar los resultados obtenidos a ficheros Word, Excel o pdf.
- Permitirá la generación de históricos para comparar la evolución del análisis y gestión de riesgos a lo largo del tiempo.
- Debe disponer de un sistema de indicadores y alertas.

- Dispondrá de un catálogo de métricas automáticas relacionadas con otras opciones de la herramienta y permitirá la definición de métricas automáticas o manuales de dicho catálogo. También contendrá indicadores que permitan evaluar los sistemas de gestión.
- Debe disponer de un módulo para la gestión de no conformidades, incidencias, acciones correctivas/preventivas y de mejora. Será posible limitar el acceso de los usuarios a la gestión de las incidencias, no conformidades, etc. Además, será posible la configuración de workflows para facilitar su gestión.
- Dispondrá de un conjunto de alertas preestablecidas que pueden ser asignadas a los empleados. El envío de las notificaciones se realizará a través de correo electrónico.
- Permitirá almacenar y controlar la documentación permitiendo la configuración tanto a nivel de carpetas como para la aprobación de la documentación
- Reporte, Cuadros de Mandos y Gestión Documental:
 - Métricas e indicadores configurables.
 - Creación de plantillas de reporte ilimitadas.
 - KPIs y objetivos de negocio.
 - Gestión documental con ciclo de vida del documento y flujos de trabajo.
 - Reportes específicos.
- Funcionalidades “Gestión de Riesgos”: *
 - Normativas y estándares soportados: ISO 31000, MEHARI, EBIOS, OCTAVE, entre otras.
 - Riesgos:
 - Seguimiento y evaluación de procesos.
 - Análisis de riesgos adaptable a cualquier metodología.
 - Evaluación de riesgos, mapas y dashboards automáticos.
 - Plan de tratamiento y gestión de riesgos con flujos de trabajo.
 - Identificación de amenazas y vulnerabilidades.
 - Realización de test de elementos, activos, riesgos y controles.
 - Definición y monitorización de KRIs.
 - Históricos ilimitados.
 - Cumplimiento:
 - Precarga de catálogos de normativas.
 - GAP Análisis.
 - Plan de adecuación automático con flujo de trabajo.
 - Evidencias de cumplimiento centralizadas.
 - Cuestionarios de cumplimiento.
 - Comparativas entre periodos.
 - Histórico de cumplimiento.
 - Gestión de Incidentes y PDCA:
 - Gestión de incidencias personalizable con flujos de trabajo.
 - Gestión de eventos de Pérdida con flujos de trabajo.
 - Gestión de riesgos en tiempo real.
 - Gestión de no conformidades, acciones correctivas y/o preventivas.

- Evaluación de proveedores.

4.- INTEGRACIÓN

Se valorará la existencia de APIs o WebServices que permitan sincronizar la solución presentada y el software que Txinzer utilice para el control de ejecución de tareas, con el objeto de sincronizar los estados de las acciones generadas en la aplicación y las tareas que impliquen dichas acciones.

En caso de no existir las mencionadas, se valorarán las propuestas de desarrollo de las mismas.

5.- SERVICIOS DE SOPORTE Y MANTENIMIENTO

El servicio de soporte y mantenimiento deberá incluir, como mínimo, lo siguiente:

- Asistencia por correo electrónico.
- Actualizaciones funcionales, correctivos y evolutivos, incluyendo cambios normativos.
- Mantenimiento de la solución a través de conexión remota.
- El fabricante se hará cargo de actualizar la solución desplegada cuando se publiquen nuevas actualizaciones de la solución.
- El horario del soporte deberá ser al menos el siguiente: de 9:00 a 17:00 en días laborales.

6.- SERVICIO DE CONSULTORÍA DE EMPRESA LICITADORA Y FABRICANTE

Se establece, para actividades rutinarias, una bolsa de 3.500.- euros anuales máximos a consumir en servicios de Consultoría de un consultor de la empresa licitadora, así como de la empresa fabricante (para el supuesto que fuera necesario), especializados en la solución, bajo demanda y sin compromiso de consumo por parte de TXINZER con los importes máximos (precio/hora) identificados en el PCAP.

Las empresas licitadoras deberán incluir en la oferta, el importe del precio hora como mínimo para estos perfiles:

- Consultor.
- Técnico desarrollador de Integración de API.

7.- PLAN DE FORMACIÓN

Los licitadores deberán incluir un plan de formación completo con definición de perfiles, roles de la aplicación, alcance de la formación para cada uno de los roles

definidos, metodología, etc. en las Propuesta Técnicas que deberán incorporar al Archivo Electrónico nº DOS de su oferta.

En Irun a febrero de 2024.