SEGURTASUN SAILA
Administrazio eta Zerbitzuen Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD
Viceconsejería de Administración y Servicios
Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

MIGRACIÓN PORTAL Y APLICACIONES AFINES

PLIEGO DE PRESCRIPCIONES TÉCNICAS

TABLA DE CONTENIDOS

Página

1. ANTECEDENTES Y OBJETO DEL PLIEGO 2

2. ALCANCE DEL CONTRATO 3

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS 4

3.1. PORTAL AFINES 4
3.2. MIGRACIÓN DE APLICACIONES 5

4. EJECUCIÓN DEL CONTRATO 8

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 8
4.2. ENTORNO TECNOLÓGICO 8
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 9
4.4. GESTIÓN DE LA CALIDAD 11
4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 14
4.6. REGISTROS, NOTIFICACIONES E INVENTARIOS. 14
4.7. LUGAR DE EJECUCIÓN DEL CONTRATO. 14

DOCUMENTOS ANEXOS 15

ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN. 15

1. ANTECEDENTES Y OBJETO DEL PLIEGO

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos (en adelante DGTSI) es la encargada de prestar servicios informáticos y de comunicaciones al Departamento de Seguridad del Gobierno Vasco.

La DGTSI, en su objetivo constante de modernización y mejora continua de las infraestructuras de comunicaciones del Departamento de Seguridad, ha elaborado unos planes de migración hacia tecnologías y servicios más actuales de productos y servicios informáticos que van dirigidos a la ciudadanía y a los diferentes sectores de la administración.

El Departamento de Seguridad cuenta con un portal web dirigido a las Policías Locales de Euskadi para ofrecer el soporte necesario para atender a las necesidades de coordinación derivadas de la Ley 15/2012, de 28 de junio, de Ordenación del Sistema de Seguridad Pública de Euskadi.

El presente pliego tiene como objetivo la migración del portal Afines y las aplicaciones que se incluyen, hacia las tecnologías y productos marcados sobre los planes de renovación tecnológica.

De acuerdo con estas necesidades se determinan las condiciones generales y particulares a las que debe ajustarse el desarrollo de esta migración, que constituyen la base para la petición de ofertas.

El presente pliego de prescripciones técnicas (P.P.T.) tiene como finalidad determinar el alcance de la prestación del servicio a realizar, así como las características generales y particulares y condiciones de ejecución a las que deben ajustarse el servicio solicitado.

2. ALCANCE DEL CONTRATO

El presente expediente tiene por objeto la contratación de las tareas de análisis, diseño, construcción e implantación del nuevo portal de Afines y la migración de las aplicaciones y contenidos del actual portal a los estándares marcados por la DGTSI.

Antes de abordar su desarrollo, la DGTSI deberá aprobar la propuesta de trabajo presentada por la empresa adjudicataria con la planificación de los trabajos aportada a los requisitos planteados en el presente PPT.

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS

3.1. Portal Afines

El nuevo portal Afines del Departamento de Seguridad se construirá bajo la plataforma Liferay DXP y estará securizado por usuarios y roles administrados sobre el sistema de seguridad corporativo.

Entre las características básicas del nuevo portal y las aplicaciones que lo integran destacan:

- **Seguridad:**
  Aquellos servicios expuestos y limitados por la seguridad restringirán el acceso en función del usuario conectado.
- **Rendimiento:**
  Los tiempos de respuesta de las peticiones realizadas deberán mantener o mejorar los actuales.
- **Multilingüismo:**
  Ha de contemplar la posibilidad de selección del idioma de navegación (Euskera o Castellano).
- **Accesibilidad:**
  La aplicación de portal cumplirá con los estándares tecnológicos y los requerimientos de accesibilidad establecidos por la DGTSI.
- **Servicios:**
  La aplicación de portal se integrará con los servicios horizontales definidos según necesidades del análisis.
- **Responsive:**
  El portal usará los estándares para garantizar su accesibilidad con independencia del dispositivo desde el cual se realice el acceso
- **Usabilidad:**
  La nueva aplicación de portal deberá seguir el libro de estilos euskadi.eus.
- **Navegadores:**

Se deberá garantizar que sea accesible desde el navegador Internet Explorer 11, Microsoft Edge, Google Chrome versión 69 y superiores, y Mozilla Firefox 65 y superiores y, aconsejable, Opera.

3.2. Migración de aplicaciones

3.2.1 Arquitectura de las aplicaciones

El actual portal Afines basado en IBM WebSphere Portal Server v8.5 integra contenidos y aplicaciones (portlets) que permiten el acceso a servicios de negocio del servidor de aplicaciones IBM WebSphere Application Server v8.5, que acceden a los datos propios de cada una de las aplicaciones.

El portal privado de Policías Locales accesible por certificado digital de agente así como por certificado Izenpe, engloba las aplicaciones y contenidos para el colectivo de las Policías Locales de la CAPV así como otros trabajadores adscritos al Ayuntamiento del municipio en el que prestan servicio.

La nueva arquitectura de aplicaciones del portal basada en Liferay DXP como producto de presentación y WebLogic como servicios de negocio, requerirá una migración de los componentes visuales y de negocio hacia el nuevo escenario.

3.2.2 Relación de aplicaciones y contenidos

- **Registro de Policías Locales**. Conjunto de aplicaciones de registro de las Policías Locales de la CAPV (Agentes, Policía local, Ayuntamientos, Informes)
- **Asignación de Talkies**. Establecimiento diario en cada centro policial la relación de cada agente con su correspondiente talky.
- **Consultas**. Servicios de consulta para la labor operativa de los agentes (Personas y Vehículos, Datos Grabación de voz, Datos Localización los recursos TETRA, Rastros)
- **Evidencias de la Policía Científica**. Gestión para la labor de la Policía Científica (Autorizaciones, Maestros, Solicitudes).

- **Ley de Seguridad Ciudadana**. Introducción y envío al Departamento de Seguridad, de las denuncias por infracciones de la Ley Orgánica sobre Protección de la Seguridad Ciudadana, así como los informes oportunos para su posterior incoación y resolución.
- **Envío de Datos Estadísticos.** Envío de datos de accidentes de tráfico, delincuencia y campañas de tráfico al Departamento de Seguridad.
- **Informes Estadísticos**. Integración con los informes para la analítica de datos.
- **Registro de Víctimas de accidentes de Tráfico de Euskadi.** Registro de los accidentes, los vehículos y las personas implicadas en estos accidentes atendidos por las Policías Locales.
- **Valoración VD/GV**. Registro de las respuestas al cuestionario de cada presunta víctima de VD/VG y así obtener la valoración de riesgo VD/VG que le permita tomar las medidas de actuación oportunas.
- **Dossieres de prensa**. Consulta de dossieres proporcionados desde el proveedor de este servicio en el ámbito de las policías locales.
- **Mensajes**. Servicio de mensajería que proporciona una herramienta para el envío y recepción de mensajes, por parte de los usuarios de Policías Locales como por los usuarios de la Dirección de Coordinación de Seguridad.
- **Avisos**. Publicación de avisos que sean de interés respecto de personas o vehículos, los cuales serán mostrados a los destinatarios de los mismos al realizar la consulta de la persona o del vehículo.
- **Siapol Aranzadi**. Integración a la base de datos de La Editorial Aranzadi que permite la prestación de un servicio de apoyo a la actividad policial basado en la definición y consulta de procedimientos actualizados de referencia para la actuación de la policía del País Vasco.

Las aplicaciones consumen servicios horizontales de gestión documental integrados sobre un Bus de integración corporativo Oracle Service Bus, que deberán modularse mediante el estándar OSGi r6 para recopilar pequeños componentes reutilizables y cooperativos.

- **Contenidos**

Existen contenidos públicos que además de publicarse es este portal son accesibles desde la página web de udaltzaingoa.euskadi.eus. Sin embargo, existen otros de carácter privado que sólo se visualizan desde la parte privada.

- **Información general.** Presentación del portal, Convenios de colaboración, Procedimientos de actuación, Uniformidad y signos distintivos, Normas gráficas para vehículos, Diplomas al servicio policial, Guías de usuario
- **Legislación:** Recopilación amplia de normas de interés policial para el desarrollo del trabajo como agente de policía, con normativa penal, de la Ley de Enjuiciamiento Criminal de tráfico, de protección civil y emergencias, seguridad ciudadana.
- **Transparencia:** Acceso a proyectos normativos y entidades de Participación Euskadi.eus**.**
- **PGSPE 2014-2019:** Plan General de Seguridad Pública de Euskadi 2014-2019.
- **Noticias:** Acceso a noticias de interés para el colectivo de policías Locales.
- **Bolsas:** Reglamento y procedimiento e histórico de bolsas de trabajo.

4. EJECUCIÓN DEL CONTRATO

4.1. Planificación y organización

El adjudicatario deberá presentar un programa de trabajo ajustado a lo prescrito en este pliego y conteniendo cuantos aspectos complementarios sobre la forma de realización de cada una de las tareas descritas en el mismo se consideren oportunas, detallando las actividades y la organización de los recursos humanos ofertados. Asimismo, deberá presentar el correspondiente Diagrama temporal de actividades (cronograma de tareas).

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible, permitiéndonos priorizar las tareas más importantes y urgentes.

4.2. Entorno tecnológico

La solución a los requerimientos recogidos en el presente pliego ha de ir alineada con la política de la DGTSI en lo que a desarrollos Java EE hace referencia.

La DGTSI proporcionara a la empresa adjudicataria toda la información necesaria para el desarrollo de este pliego en el nuevo entorno tecnológico.

Dicho entorno se basa en una arquitectura orientada a servicios (SOA), en la que se exponen distintos tipos de servicios, apoyados en un Framework de desarrollo Java EE y cuya presentación se implementa sobre el nuevo portal “Afines”.

Con carácter general se encuentran establecidos tres niveles o entornos de ejecución de las aplicaciones: Desarrollo, Preproducción o Formación y Producción.

Se deberá garantizar que la aplicación dentro del portal Afines pueda ser accesible desde el navegador Internet Explorer 11, Microsoft Edge, Google Chrome versión 69 y superiores, y Mozilla Firefox 65 y superiores y, aconsejable, Opera.

A lo largo de la vida del contrato pueden cambiar tanto las versiones como los productos que se citan.

Gestión de portales y Servidor de aplicaciones:

- Desarrollo de Portlets sobre JBoss 7.1 y Liferay DXP 7.1
- Desarrollo de EJBs sobre Oracle WebLogic Server 12.2.1.4

Gestión documental:

- IBM DB2 Content Manager v8.4

Bus de integración de servicios y aplicaciones:

- Oracle Service Bus 12c

Servidor de Bases de datos:

- DB2 z/OS v.11
- Oracle 12 RAC

Repositorio de código fuente:

- Azure DevOps Server 2019

Repositorio Documental de Proyecto:

- Microsoft SharePoint 2010.

Frameworks y estándares:

- Todos los desarrollos deben realizarse para la versión 8 de la JDK
- Frontend: Portlet 3.0 (JSR-362), Liferay MVC Portlet, JSF 2.2 (JSR 286), Bundles OSGi R6
- Backend: EJB 3.2, JPA 2.1
- La DGTSI dispone de un conjunto de servicios horizontales y componentes reutilizables para dar solución a las necesidades comunes identificadas por las aplicaciones.

4.3. Cualificación técnica del equipo de trabajo

La empresa deberá tener personal técnico con la formación necesaria que incluirá al menos los siguientes perfiles:

Jefe de Proyecto

- En colaboración con el técnico responsable DGTSI, se encargará de la gestión operativa del proyecto, coordinando al equipo de trabajo definido para el desarrollo del proyecto.
- Se encargará de la gestión del plan y del aseguramiento de la calidad del Proyecto
- Se responsabilizará de las tareas de análisis y diseño de la arquitectura funcional y tecnológica de la solución, así como de definir su configuración y despliegue.
- Será el soporte técnico de alto nivel para todo el equipo de trabajo, sobre la plataforma, orientando las soluciones óptimas a las necesidades que puedan plantearse, tanto desde el punto de vista técnico como funcional.
- Colaboración con el equipo de la DGTSI, para orientar las soluciones óptimas a las necesidades que dicho equipo plantee a nivel de infraestructura y plataforma base.

Analista / Desarrollador

- Elaboración de las especificaciones técnicas de la solución.
- Realización de mantenimiento correctivo y evolutivo sobre los desarrollos necesarios para dar solución a funcionalidades específicas, así como las validaciones necesarias que garanticen su calidad.
- Preparación de despliegues en los entornos del Departamento de Seguridad
- Preparación técnica y documental de los paquetes de versión necesarios para la implantación de las versiones necesarias.

4.4. Gestión de la calidad

La DGTSI establece los procedimientos de calidad definiendo aquellas pautas necesarias que logren un aseguramiento de la calidad de procesos, productos y servicios y evalúe de forma objetiva las actividades software enmarcadas en el presente contrato.

Con objeto de mejorar progresivamente la calidad del software incluida en el ámbito del presente pliego de bases técnicas, el adjudicatario deberá realizar las tareas definidas en el Plan de Calidad del Departamento de Seguridad. Entre los aspectos a contemplar estarán los siguientes:

- Controles de calidad para los entregables (documentación) que se hayan visto afectados.
- Pruebas unitarias que evite la introducción de un nuevo defecto al intentar reparar el inicialmente o la reparación incorrecta del error que se pretendía corregir.
- Pruebas de integración. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.
- Pruebas de sistema. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.
- Pruebas de carga o rendimiento, en los casos, que se establezcan en función de la modificación realizada.

El equipo de Aseguramiento de la Calidad evaluará a su vez los procesos productivos del proyecto asegurando que la información presentada es correcta, se realizan las entradas y salidas adecuadas de cada proceso, los documentos apropiados son actualizados y se aplica un sistema para recoger, revisar y seguir las acciones correctoras hasta su cierre.

Se identificarán y documentarán las no conformidades localizadas y se asegurará que las no conformidades son tratadas retroalimentando así la mejora continua del producto y los resultados de las actividades de aseguramiento de la calidad. No se dará por válida la solución y documentación entregada hasta que se corrijan las posibles deficiencias que pudieran detectarse.

El número de no conformidades tanto menores como mayores que superen el nivel de cumplimiento exigido podrá llevar asociado la aplicación de penalizaciones, salvo justificación pormenorizada del proveedor en la revisión, y aceptación de la misma por parte del responsable de la Dirección General de Telecomunicaciones y Sistemas Informáticos que se defina a tal efecto.

Los productos entregables que se revisarán durante los procesos de auditoría de Calidad son de código fuente y documental tanto de proyecto como de producto.

El proyecto y los productos entregables asociados seguirán una metodología de desarrollo iterativo basada en entregas más cortas pero funcionales y operativas desde su primera entrega e incrementales en el tiempo.

Durante las diferentes iteraciones definidas del proyecto, herramientas y plantillas tipo facilitarán la cumplimentación de información por cada entregable.

a) Proyecto

- Planificación y seguimiento del proyecto haciendo uso de las herramientas y plantillas de gestión definidas por normativa.

b) Producto

- Documento de requisitos con la identificación de los requisitos funcionales/no funcionales del Sistema.
- Casos de Uso con la definición de las secuencias de interacciones (pasos/actividades) que deberán realizarse para llevar a cabo entre los procesos del sistema y sus actores.
- Arquitectura del sistema con el diseño a de la arquitectura y descripción de los componentes de la arquitectura junto sus relaciones.
- Diseño físico de datos con el esquema físico de la base de datos, descripción de los objetos utilizados y volumetría estimada de las tablas e índices de BBDD
- Plan de Pruebas con la relación de los casos de prueba, descripción de los pasos y resultados esperados.

- Migración y carga Inicial, identificando los procesos necesarios para la migración de datos y/o cargas iniciales.
- Análisis de clases con las entidades para cada subsistema, especificando las responsabilidades que tienen asociadas, sus atributos y las relaciones entre ellas.
- Manual de explotación que recogerá el conjunto de tareas que se deberán realizar para la correcta explotación del sistema.

Todos los elementos producto del desarrollo y ejecución del contrato deberán quedar albergados en los servidores corporativos del Departamento de Seguridad, con la estructura que se habilitará al efecto y cumpliendo con las normativas internas definidas salvo que se indique expresamente lo contrario. Esto incluye código fuente, archivos binarios, ejecutables, contenidos estáticos, scripts de cualquier tipo (creación o adaptación de base de datos, construcción y empaquetado del producto, etc.), ficheros de configuración, certificados, etc., así como toda la documentación asociada: planificación, requisitos, análisis, diseño, pruebas, implantación; manuales de uso, mantenimiento, configuración, construcción y empaquetado; actas de reunión, informes de avance, etc. En cualquier momento del desarrollo y ejecución del contrato se podrá solicitar a la empresa adjudicataria la entrega de cualquier o todos estos elementos para su validación y control.

4.5. Normas de seguridad relativas a los sistemas de información

La empresa adjudicataria se compromete a cumplir las normas respecto a los sistemas de información del DSGV recogidas en el Anexo 1: Normas de seguridad relativas a los sistemas de información.

4.6. Registros, notificaciones e Inventarios.

Como parte del contrato, la empresa adjudicataria estará obligada a dar total cumplimiento a las condiciones que al efecto de control establezcan el técnico o técnica del Gobierno Vasco.

La empresa adjudicataria deberá proporcionar la información requerida por el Gobierno Vasco para conocer la situación y desarrollo de los servicios contratados. Esta información se proporcionará en forma de informes que deberán presentarse de forma periódica.

La elaboración de estos informes periódicos tiene carácter obligatorio y será entregado al técnico o técnica responsable del Gobierno Vasco junto con la facturación.

4.7. Lugar de ejecución del contrato.

El lugar de trabajo, por defecto, serán las instalaciones que determine y disponga la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos en su sede de Larrauri Mendotxe bidea, 18 en Erandio (Bizkaia).

DOCUMENTOS ANEXOS

Anexo 1. Normas de seguridad relativas a los sistemas de información.

La empresa adjudicataria se compromete a cumplir las siguientes normas de comportamiento respecto a los sistemas de información del Departamento de Seguridad del Gobierno Vasco:

- No introducir software informático ajeno al Departamento de Seguridad del Gobierno Vasco
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del Departamento de Seguridad del Gobierno Vasco, ni la documentación que se le suministre o la que pudiera tener acceso en el desempeño de sus funciones, con independencia del soporte en que se encuentre contenida.
- Acceso exclusivo a la información necesaria para el desempeño de las funciones encomendadas.
- Utilizar exclusivamente la password-clave que se le ha asignado y adquirir el compromiso de actuar de forma cuidadosa para que nadie conozca su palabra de paso.
- Utilizar adecuadamente y de forma cuidadosa los sistemas de seguridad implantados, de forma que se respeten y mantengan los niveles de seguridad.
- No utilizar el sistema de correo u otro medio alternativo para sacar fuera de la organización la información a la que se tenga acceso en el desempeño de sus funciones.

Además, la empresa adjudicataria adquirirá los siguientes compromisos, que a continuación se describen en cuanto a materia de seguridad se refiere:

- Los equipos conectados a la red corporativa del Departamento de Seguridad del Gobierno Vasco no podrán conectarse a ningún sistema informático o de telecomunicaciones ajeno al Departamento.
- Los equipos o sistemas que por su actividad requieran conexión a servicios externos al Departamento deberán estar aislados, es decir, separados física y lógicamente de la red informática del Departamento de Seguridad del Gobierno Vasco

- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del Departamento de Seguridad del Gobierno Vasco.

1 Acceso y protección de datos

La empresa adjudicataria quedará expresamente obligada al cumplimiento de lo dispuesto en la normativa (1) establecida en materia de protección de datos de carácter personal, así como de la establecida para la seguridad de la información. En este sentido, la empresa adjudicataria quedará sujeta a las obligaciones establecidas en la Política de Seguridad de la Información del Departamento de Seguridad y su Normativa de Seguridad, debiendo adoptar las medidas técnicas y organizativas que garanticen un tratamiento conforme con los requisitos de dicha normativa que permita además asegurar la disponibilidad, confidencialidad e integridad de los datos manejados y de la documentación facilitada, y evitar su pérdida, alteración o acceso no autorizado.

En particular, deberá mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en el contrato, acto jurídico o Pliego de Prescripciones Técnicas, ni tampoco ceder a otros ni siquiera a efectos de conservación. A estos efectos, deberán establecerse las máximas cautelas en el acceso a los datos. Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales, o de otro tipo, en que se puedan incurrir.

Cuando algún aspecto de la citada Política de Seguridad no pueda ser satisfecho será previa y debidamente informado para evaluar y gestionar las medidas que resulten oportunas. Asimismo, con ocasión de eventuales incidencias que pudiesen acontecer, se hará uso de los específicos procedimientos establecidos de reporte y resolución de las mismas.

Ante un incumplimiento se actuará conforme a lo establecido en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, sin perjuicio de las acciones reflejadas en los pliegos de contratación, o cualquier otra acción que se determine en base a la naturaleza y gravedad del hecho.

(1) *Normativa: 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Directiva (UE) 2016/680 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Esquema Nacional de Seguridad.*

2 Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán a la Administración. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito de la Administración.

Asimismo, todos los entregables que deban facilitarse a los Departamentos y Organismos Autónomos del Gobierno Vasco (salvo las ofertas previas) únicamente deberán llevar como logotipo o señas de identidad el escudo del Gobierno Vasco o logotipos aceptados por el propio Departamento y Organismo Autónomo.

La empresa adjudicataria se verá también obligada a guardar las normas vigentes sobre, Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vea obligado a manejar.