EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA
Administeta Zerbitzuen Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak
Kudeatzeko Zuzendaritza

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

APLICACIÓN REGISTRO Y GESTIÓN DEL INTERCAMBIO DE INFORMACIÓN POLICIAL

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Larrauri Mendotxe bidea, 18 – 48950 ERANDIO (Bizkaia)
Tel. 94 607 80 00 – Fax 94 607 83 02

TABLA DE CONTENIDOS

Página

1. ANTECEDENTES Y OBJETO DEL PLIEGO 2
2. ALCANCE DEL CONTRATO. 3
3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS. 4
4. EJECUCIÓN DEL CONTRATO 7
   - 4.1. PLANIFICACIÓN Y ORGANIZACIÓN 7
   - 4.2. ENTORNO TECNOLÓGICO 7
   - 4.3. EQUIPO DE TRABAJO: PERFILES Y FUNCIONES 8
   - 4.4. GESTIÓN DE LA CALIDAD 9
   - 4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 12
   - 4.6. REGISTROS, NOTIFICACIONES E INVENTARIOS. 12
   - 4.7. LUGAR DE EJECUCIÓN DEL CONTRATO. 12

DOCUMENTOS ANEXOS 13

ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN. 13

1. ANTECEDENTES Y OBJETO DEL PLIEGO

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos es la encargada de prestar servicios informáticos y de comunicaciones al Departamento de Seguridad del Gobierno Vasco. En dicho contexto, y en lo que atañe al desarrollo de los sucesivos planes de Gestión de Sistemas, debe abordar una serie de proyectos para la construcción y mantenimiento de los sistemas de información que pone a disposición de sus usuarios.

Desde la Sección de Cooperación Policial y Judicial del Departamento de Seguridad se comunicó a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos la necesidad de renovación de su aplicación, para la mejora de la gestión del intercambio de información.

El objetivo del nuevo Sistema de información es proporcionar a la Sección de Cooperación Policial y Judicial del departamento de Seguridad una herramienta para el registro y gestión del intercambio de información con otros organismos o estamentos, principalmente cuerpos policiales tanto estatales como extraestatales. Este nuevo sistema se incluirá como un nuevo módulo de Gurenet dentro de la sección Área de Trabajo.

El objeto de este expediente es la contratación del desarrollo para la ejecución de los trabajos necesarios, definición, diseño, construcción e implantación, según se detallan a lo largo de este pliego, para el nuevo desarrollo del aplicativo de registro y gestión del intercambio de información policial.

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.

Actualmente existe una aplicación cliente Access para el registro y gestión del intercambio de información con otros organismos o estamentos. Esta aplicación además de tener limitaciones está dando una serie de problemas de rendimiento.

El alcance del proyecto es la creación de una nueva aplicación de gestión de expedientes policiales que dé solución a los problemas detectados en la aplicación Access y a los nuevos requerimientos.

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos tras reunirse en varias ocasiones con los usuarios y realizar un análisis funcional, presentó una propuesta que fue aprobada por Sección de Cooperación Policial y Judicial del departamento de Seguridad. Esta propuesta será el punto de partida para el arranque del proyecto.

Una vez finalizada e implantada la aplicación, la empresa adjudicataria se encargará de dar Soporte y mantenimiento post-implantación, con la finalidad de atender consultas y publicar nuevas versiones que sean necesarias para corregir las deficiencias que sean detectadas durante el plazo de ejecución establecido.

3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS.

El aplicativo web a desarrollar se incluirá como un nuevo módulo de Gurenet dentro de la sección Área de Trabajo y tendrá diferentes niveles de acceso, por lo que será necesario la generación de perfiles de acceso que garanticen la seguridad de la información almacenada.

Deberá proporcionar las siguientes funcionalidades:

- Registrar expedientes policiales con toda la información necesaria (datos, documentos, mails) almacenando también las reiteraciones, solicitudes a otras unidades, sus respuestas y la respuesta final.
- Permitir realizar búsquedas ágiles de expedientes policiales almacenados en el sistema, y realizar informes.
- Realizar el mantenimiento de cuantas tablas maestras sean necesarias.
- Enviar a Jefatura de sección el expediente policial para su conocimiento y que éste dictamine como proceder, así como realizar la firma del documento, preferentemente electrónica, si estuviera disponible, que irá en la respuesta final sin necesidad de trabajar con papel.
- Habrá integración con la aplicación 56.03 BUROTICA del Sistema de Información Policial (SIP), obteniendo de forma automática el número de entrada y salida de cada expediente policial.

Además de las tareas descritas, será necesario realizar la migración de los expedientes policiales almacenados en la aplicación Access existente actualmente.

El alcance del sistema contempla además los siguientes aspectos fundamentales que deberán ser llevados a cabo por el adjudicatario durante la prestación de sus servicios:

1. Afianzar el cambio tecnológico Java EE emprendido, integrando esta iniciativa con el resto de las iniciativas ya completadas.
2. Los sistemas deberán proporcionar un tiempo de respuesta adecuado, evitando las opciones de desarrollo que puedan producir retardos en el mismo. Así

mismo, deberán procurar que el entorno de trabajo sea intuitivo, y sencillo para el usuario.

3. Mejorar la calidad de los servicios y la eficiencia de los sistemas aprovechando los nuevos recursos y servicios disponibles en el propio Departamento de Seguridad y otras administraciones.
4. Conseguir una modernización de la plataforma de trabajo obteniendo una evolución continua de los desarrollos e incrementando mayor potencial a las funcionalidades actuales.
5. Aprovechar las sinergias que puedan surgir entre los diferentes proyectos (Framework de ejecución, infraestructura, procesos, servicios reutilizables, etc.).
6. Potenciar la prestación de servicios on-line.
7. Garantizar la continuidad operativa y tecnológica de las aplicaciones permitiendo flexibilidad hacia nuevos requerimientos.
8. Centralizar los servicios hacia un punto único de acceso y evitar la utilización de diversos productos y tecnologías para un mismo fin.
9. Integración del servicio web con diferentes plataformas y entornos que garanticen su uso e integración desde cualquier aplicación de Seguridad hasta la completa migración de todas ellas al nuevo entorno tecnológico.

El nuevo sistema a construir objeto del pliego deberá contemplar las siguientes características básicas:

- **Seguridad:**

  Aquellos servicios expuestos y limitados por la seguridad restringirán el acceso en función del usuario conectado.

- **Multilingüismo:**

  La nueva aplicación de portal ha de contemplar la posibilidad de selección del idioma de navegación (Euskera o Castellano)

- **Accesibilidad:**

La nueva aplicación de portal cumplirá con los estándares tecnológicos y los requerimientos de accesibilidad establecidos por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.

- **Servicios:**

  La nueva aplicación de portal se integrará con los servicios horizontales definidos según necesidades del análisis (SIP, gestor documental, concurrencia, auditoría, NORA, correo...)

- **Usabilidad:**

  La nueva aplicación de portal deberá seguir la guía de estilos que se proporcione por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.

- **Navegadores**

  Se deberá garantizar que las aplicaciones Gurenet, puedan ser accesibles desde el navegador Internet Explorer 11 y Microsoft Edge.

El sistema se integrará en la nueva plataforma tecnológica con tecnología Java EE. Dispondrá de una interfaz gráfica que se incorporará al portal de intranet Gurenet y proveerá de los servicios necesarios para resolver las peticiones y respuestas a las aplicaciones.

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.

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible.

4.2. Entorno tecnológico

Este nuevo aplicativo se integrará dentro del portal Gurenet. El desarrollo se realizará en J2EE.

Entorno de desarrollo web:

- WebSphere Portal Server 8.5
- Liferay DXP 7.1
- WebSphere Application Server 8.5
- Oracle Weblogic Server 12c
- Oracle Service Bus 12c
- IBM MQ 7.5
- Oracle RAC 12c
- DB2 z/OS v.12

El Framework será el siguiente:

- Portlets 2.0 (JSF)
- EJB 3.X
- JPA 2.X

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

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

4.3. Equipo de trabajo: Perfiles y funciones

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 Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, 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 Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos 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 de Gestión 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. Para cada una de las fases existen herramientas y plantillas tipo que facilitará cumplimentar la información para cada entregable requerido.

- Fase gestión
  - Planificación y seguimiento del proyecto haciendo uso de las herramientas y plantillas de gestión definidas por normativa.
  - Cronograma de tiempos con el detalle de actividades por fase/tarea e hitos del proyecto.
- Fase funcional
  - Documento de requisitos con la identificación de los requisitos funcionales/no funcionales del Sistema.
  - Análisis funcional con la descripción funcional del sistema e identificación de los procesos.
  - 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.
- Fase técnica
  - 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 y descripción de los objetos utilizados.

- Volumetría del volumen estimado de las tablas e índices de BBDD
- Interface de usuario con el diseño de los interfaces de usuario necesarios para el sistema.
- 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 identificando las entidades para cada subsistema, especificando las responsabilidades que tienen asociadas, sus atributos y las relaciones entre ellas.

• Fase Implantación
  - Manuales de usuario según perfil
  - 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 de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

- No introducir software informático ajeno a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, 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 de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos 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 de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.
- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del Departamento de Seguridad.

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 función de su ámbito de aplicación y de su no exclusión por tratarse de información clasificada sujeta a la regulación de Secretos Oficiales y normas de desarrollo. 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.*

Esquema Nacional de Seguridad, en lo relativo a lo que establece el RD 3/2010 de 8 de enero.

Esquema Nacional de Interoperabilidad, en lo relativo a lo que establece el RD 4/2010 de 8 de enero.

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.