EXPLOTACIÓN DE DATOS PARA LAS UNIDADES TERRITORIALES DE TRÁFICO

PLIEGO DE PRESCRIPCIONES TÉCNICAS

TABLA DE CONTENIDOS

Página

1. ANTECEDENTES Y OBJETO DEL PLIEGO 2

2. ALCANCE DEL CONTRATO 4

3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS. 5

3.1. TAREAS DE CARGA DE DATOS 5
3.2. CREACIÓN DE INFORMES 5

4. EJECUCIÓN DEL CONTRATO 7

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 7
4.2. ENTORNO TECNOLÓGICO 7
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 8
4.4. GESTIÓN DE LA CALIDAD 8
4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 11
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

El Departamento de Seguridad del Gobierno Vasco, a partir de ahora DSGV, dispone de un sistema de inteligencia empresarial y almacenamiento de datos, dividido en diferentes conjuntos conceptuales, que permiten profundizar en el análisis de datos para la toma de decisiones.

Las tres Unidades Territoriales de Tráfico de la Dirección de la Ertzaintza elaboran una serie de informes y cuadros de mando con información referente a los Accidentes de Tráfico ocurridos en la CAE junto con la actividad policial realizada en los distintos Controles Preventivos de Tráfico, que sirven de soporte a las distintas reuniones del Consejo de Unidad, Territoriales y Consejo Gestor Territorial. Con el objeto de modernizar esta explotación, de facilitar el cálculo de la misma y de incorporar nuevas funcionalidades, se ve en la necesidad de disponer de un proyecto que facilite a los usuarios de una forma visual rápida la información relativa a la actividad desarrollada por las Unidades Territoriales de Tráfico de la Ertzaintza, aportando principalmente información referente a:

- Siniestralidad
- Accidentalidad
- Mortalidad
- Prevención
- Denuncias

La visualización de estos datos es a través de documentos interactivos, de interfaz visual, gráfica y de manejo fácil e intuitivo.

Además de estos informes estadísticos, es necesario dotar de otros de carácter dinámico con el objetivo de que los analistas de las Unidades Territoriales de Tráfico puedan hacer sus propias consultas *ad-hoc* para satisfacer necesidades puntuales que puedan surgir para la toma de decisiones.

Para obtener estos informes, es necesario llevar a cabo desarrollos que incorporen información aún no disponible en el sistema de inteligencia empresarial del DSGV.

El objeto de este documento es detallar el alcance de los requisitos relativos a proyectos del sistema de inteligencia empresarial y explotación de datos para estadísticas y análisis del DSGV.

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 los desarrollos que se especifican a continuación:

- Desarrollos necesarios para almacenar la información que actualmente no está recogida en el repositorio de datos del sistema de inteligencia empresarial.
- Creación de informes para las reuniones del Consejo de Unidad de las Unidades Territoriales de Tráfico (UTT), reuniones Territoriales de las UTT y reuniones del Consejo Gestor Territorial
- Creación de unos Cuadros de Mando dinámicos

Antes de abordar su desarrollo, la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos 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 PBT.

Estos desarrollos deben realizarse dentro del sistema de inteligencia empresarial del DSGV y deberán coordinarse con el equipo de mantenimiento del sistema de inteligencia empresarial para tareas que requieran de su intervención.

3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS.

Para la elaboración de estas tareas será necesaria la coordinación con el equipo de mantenimiento del sistema de información empresarial, que será el encargado de la puesta en producción de todos los procesos realizados, junto con la comprobación y validación de que todos los datos sean correctos y acordes a los requerimientos recogidos.

3.1. Tareas de Carga de Datos

Al tratarse de nuevos informes, será necesario crear conjuntos de datos que actualmente no existen dentro del almacenamiento de datos del sistema de inteligencia empresarial.

Adicionalmente, será necesario preparar los procesos de extracción, transformación y carga de datos automático con la herramienta corporativa actual al sistema de inteligencia empresarial.

3.2. Creación de Informes

Consiste en la generación de nuevos documentos como soporte a las distintas reuniones que las Unidades Territoriales de Tráfico de la Ertzaintza realizan en el Consejo de Unidad, en la Territorial y en el Consejo Gestor Territorial para la toma de decisiones.

Adicionalmente, se incorporará la creación de nuevos informes dinámicos, que permitan analizar la información relacionada con la actividad realizada por las Unidades Territoriales de Tráfico de la Ertzaintza en relación con la accidentalidad en la CAE.

Las tareas a desarrollar son las siguientes:

- Creación de 16 documentos dirigidos a las reuniones de las UTT, compuestos por tablas, mapas geoespaciales y gráficos, y la incorporación de funcionalidad dinámica a través de, entre otros, pestañas, criterios de selección, botones y combos. La información correspondiente a estos documentos hace referencia a:
    - Siniestralidad
    - Accidentalidad
    - Controles Preventivos

- Denuncias
- Mortalidad

- Creación de 5 documentos de carácter interactivo, de interfaz visual y gráfico y de manejo fácil e intuitivo, que permiten a las Unidades Territoriales de Tráfico el análisis y estudio de la información *ad-hoc* para la toma de decisiones. La información correspondiente a estos documentos hace referencia a:
  - Análisis de la Accidentalidad
  - Lesividad en Carreteras
  - Circunstancias de las Vías y Factores Concurrentes
  - Accidentalidad por día del mes, de la semana y franja horaria
- Proporcionar la seguridad correspondiente a los informes y a cada uno de sus elementos dependientes.

Para la elaboración de estas tareas será necesaria la incorporación adicional de atributos, hechos, indicadores y filtros además de los informes y documentos descritos dentro del sistema de inteligencia empresarial, así como la integración de tablas en el almacenamiento de datos.

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 que intervendrán en la ejecución del contrato. 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, permitiendo el correcto ajuste temporal de todas las tareas que constituyen el contrato.

4.2. Entorno tecnológico

La solución a los requerimientos recogidos en el presente pliego ha de ir alineada con la política de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos en lo que a desarrollos del sistema de inteligencia empresarial hace referencia.

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos proporcionará a la empresa adjudicataria toda la información necesaria para el desarrollo de este pliego en el nuevo entorno tecnológico.

Con carácter general se encuentran establecidos dos niveles o entornos de ejecución de los proyectos: Desarrollo y Producción.

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

La arquitectura tanto en Desarrollo como en Producción para estos proyectos, es la siguiente:

- Carga y almacenamiento de datos en el sistema de inteligencia empresarial:
  - Entorno: Linux
  - La herramienta ETL: IBM InfoSphere DataStage es la 11.3.1

- Base de Datos: DB2 con Acelerador Blu
- Ficheros planos

- Explotación de datos del sistema de información empresarial:
  - MicroStrategy 2020
- Repositorio de código fuente
  - Microsoft Visual Studio 2010
- Repositorio Documental de Proyecto
  - Microsoft SharePoint 2010

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:

2 Analistas / Desarrolladores

- Elaboración de las especificaciones técnicas de la solución, así como preparación de su despliegue en los entornos del Departamento de Seguridad
- Realizarán desarrollo y pruebas sobre las funcionalidades específicas sobre el sistema de inteligencia empresarial, tanto de los procesos de ETL como de los cubos de inteligencia y de los informes y documentos necesarios para dar solución a los requerimientos establecidos
- 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 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. 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.
- 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 con la definición de las métricas utilizadas
  - 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 la ejecución del contrato. Esta información se proporcionará en forma de informes que deberán presentarse de forma periódica, y a través de la herramienta de gestión que para tal fin se defina.

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*

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.