EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA
Babes Zibileko Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD
Viceconsejería de Protección Civil
Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

GESTIÓN DE COMUNICACIONES DE VUELOS DE UAS

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 LAS FUNCIONALIDADES REQUERIDAS 5

3.1. GESTIÓN DE LAS COMUNICACIONES DE VUELOS DE UAS 5
3.2. MANTENIMIENTO DE DATOS MAESTROS 11
3.3. ZONAS RESTRINGIDAS. 12
3.4. ÁREA DE ANÁLISIS DE COMUNICACIONES DE VUELOS DE UAS. 12
3.5. INTEGRACIÓN CON EL SISTEMA DE GESTIÓN INCIDENTAL 13
3.6. CONSIDERACIONES ADICIONALES 13

4. EJECUCIÓN DEL CONTRATO 16

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 16
4.2. ENTORNO TECNOLÓGICO. 16
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 19
4.4. GESTIÓN DE LA CALIDAD 19
4.5. DOCUMENTACIÓN NO SEXISTA 23
4.6. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 23
4.7. REGISTROS, NOTIFICACIONES E INVENTARIOS. 23

DOCUMENTOS ANEXOS 24

ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN. 24

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 (DSGV).

Desde la Secretaría General de la Ertzaintza surge la necesidad de gestionar de manera eficiente las comunicaciones de vuelos de Sistemas Aéreos no Tripulados, en adelante UAS. Estas comunicaciones se reciben por diferentes cauces, y es necesario recoger la información de las operadoras, pilotos, operaciones, observadores y UAS, además de la documentación asociada. La gestión de estas comunicaciones conlleva la coordinación de las diferentes unidades policiales implicadas y las valoraciones de las mismas sobre la posible afección de estos vuelos en la seguridad pública. Para ello la nueva aplicación deberá integrarse con el sistema de información policial, el sistema de gestión incidental, la sede electrónica y la cartografía corporativa.

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

El objeto de este expediente es la contratación de los servicios para la construcción e implantación del Sistema de Gestión de Comunicaciones de Vuelos de UAS.

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 de la aplicación para la Gestión de Comunicaciones de Vuelos de UAS, facilitando la recogida y mantenimiento de los datos de operadoras, pilotos, observadores, operaciones y UAS, que se deben hacer constar en las comunicaciones. Se debe tener en cuenta que las comunicaciones de vuelos se reciben por diferentes cauces, las comunicaciones realizadas desde sede electrónica se registrarán automáticamente y, además, la aplicación permitirá el registro y mantenimiento de las comunicaciones recibidas por otros cauces. En la aplicación se deben contemplar también las valoraciones, informes y controles de las diferentes unidades policiales implicadas. Todo ello integrado con el sistema de gestión incidental y la cartografía corporativa. Dicho desarrollo se presta como una unidad funcional por lo que no procede la división en lotes del contrato.

Las funcionalidades a nivel general que debe cubrir la aplicación objeto de este contrato son las siguientes:

a) El registro y mantenimiento de los datos de: comunicaciones, operadoras, pilotos, observadores, UAS y operaciones, además de la documentación asociada a cada una de estas entidades. Teniendo en cuenta que las comunicaciones se reciben por diferentes cauces y las comunicaciones realizadas en sede electrónica se cargarán automáticamente.

b) Informar a las diferentes unidades policiales implicadas en cada caso: Comisarías, Territoriales, Unidad de Vigilancia Rescate (UVR), Gabinete Técnico (GT), Jefatura de la Oficina Central de Inteligencia (JOCI) y Ardatz Central.

c) Incorporar las valoraciones, informes y aportaciones de las diferentes unidades policiales implicadas, según los plazos establecidos.

d) Realizar los controles automáticos requeridos, entre ellos los referidos a áreas restringidas, detectando solapes entre estas áreas y las zonas de vuelo.

e) Trasladar al sistema de gestión incidental la información sobre vuelos planificados.

f) Consultar las comunicaciones tanto pendientes como resueltas y toda la información asociada.

g) Visualizar en la cartografía corporativa el conjunto de zonas de vuelos de drones comunicados, según los criterios de selección.

h) Registro y mantenimiento de las zonas restringidas para los vuelos, debido a la existencia de infraestructuras sensibles u otras causas.

i) Controlar en base al perfil de usuario que accede a la aplicación si puede consultar, crear, valorar o finalizar las comunicaciones y realizar el mantenimiento de: operadoras, pilotos, observadores, operaciones, UAS, comunicaciones y documentos asociados; así como el mantenimiento de zonas restringidas.

j) Análisis de datos en Cuadros de Mando Bussiness Intelligence: Este módulo presentará los Cuadros de Mando analíticos que explotarán los datos estadísticos relacionados con las comunicaciones de vuelos de UAS.

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS

Con la finalidad de facilitar una gestión eficiente de las comunicaciones de vuelos de UAS, la aplicación ofrecerá las siguientes funcionalidades:

3.1. Gestión de las Comunicaciones de Vuelos de UAS

Para la gestión de las Comunicaciones de Vuelos la aplicación dispondrá de los siguientes módulos:

3.1.1 Comunicación de Vuelos de UAS

En este bloque se registran y mantienen los datos propios de la Comunicación. La información básica que incorporan las Comunicaciones será del tipo:

- Número Comunicación: El formato de este número será AAAA/XXXXX, donde AAAA será el año del expediente y XXXXX será un número incremental.
- Referencia Tramitagune: Para las comunicaciones que se registran automáticamente desde Sede Electrónica, este campo representa a la referencia que le asigna Sede Electrónica a la comunicación.
- Referencia Ministerio: Para las comunicaciones que llegan desde el Ministerio del Interior, este campo representa a la referencia que el Ministerio asigna a la comunicación.
- Fecha y Hora del registro de la comunicación.
- Estado de la Comunicación.
- Documento de la Comunicación: para las comunicaciones que vienen de Sede Electrónica, se tendrá cargada la comunicación que envía el comunicante. Para el resto de comunicaciones que se registran manualmente en la aplicación, se podrá adjuntar la solicitud de vuelo que se haya recibido por otros cauces.
- Observaciones: para aportar a la comunicación la información adicional que se considere oportuna.

3.1.2 Datos de la Operadora

En este apartado se incluirá la información relativa al Operador que comunica el vuelo. En las comunicaciones que se registran desde Sede Electrónica los datos se cargarán automáticamente.

Los datos a registrar y mantener se detallan en 3.2.1 Mantenimiento de Operadoras.

En caso de que no exista la Operadora (por tipo-número documento) en las tablas maestras de la aplicación, se facilitará la incorporación de los datos de la nueva Operadora en las tablas maestras mediante un botón “Añadir”. Pulsando este botón emergerá una pantalla que se cargará con los datos de la Operadora que viene en la comunicación. Pulsando el botón “Guardar” de la pantalla emergente se dará de alta en las tablas maestras de la aplicación la nueva Operadora.

En caso de que la Operadora ya se encontrase dada de alta en las tablas maestras de la aplicación (existe ya una Operadora con ese tipo-número de documento) en la parte superior derecha del módulo aparecerá un botón de tipo “Lupa”. Al pulsar el botón, emergerá una pantalla con los datos de la operadora registrados en la tabla maestra de Operadoras. De esta manera se podrán cotejar los datos almacenados en la tabla maestra con los datos que han llegado en la comunicación, y en caso de no coincidir se podrían actualizar los datos de la tabla maestra pulsando el botón “Actualizar”, que cargará los campos de la pantalla emergente con los valores de los campos de la Operadora de la comunicación. Para las comunicaciones que no vienen de sede electrónica y hay que registrar manualmente, al introducir el tipo de documento y número de documento de la Operadora, la aplicación comprobará si existe una Operadora con ese tipo-número de documento en las tablas maestras y, automáticamente, cargará el resto de datos de esa Operadora en el bloque. Y se podrá actuar de la misma manera que si hubiese llegado de sede electrónica, pudiendo actualizar los datos de las tablas maestras en caso de que no coincidan los datos de la Operadora de las tablas maestras con los datos que ha enviado la Operadora en la comunicación.

3.1.3 Datos del Piloto.

En este apartado se recogerá la información relativa al piloto que realizará el vuelo y el tratamiento a realizar con sus datos será el mismo que el descrito para la Operadora.

Los datos a registrar y mantener se detallan en 3.2.2 Mantenimiento de Pilotos.

3.1.4 Datos de la Operación.

En este bloque se registra la información relativa a la operación de vuelo del UAS, mediante datos como:

- Tipo y categoría.
- Descripción de la operación.
- Fecha y hora de inicio del vuelo.
- Fecha y hora de fin del vuelo.
- Lugar de la operación.
- Geolocalización:
    - Mapa con coordenadas, se mostrará un mapa con la cartografía corporativa de manera que al marcar un punto en el mapa rellenará las coordenadas. Dependiendo del origen de la comunicación, el formato de las coordenadas podría variar, por lo que se deberá contemplar la conversión entre diferentes formatos de coordenadas.
    - Zona de vuelo.
    - Altura.
    - Radio.
- Polígono de vuelo con las coordenadas de los vértices.

3.1.5 Datos de los UAS.

En este apartado se recogerá la información relativa al UAS y el tratamiento a realizar con sus datos será el mismo que el descrito para la Operadora y Piloto. En el caso de los UAS la identificación se hará por el número de serie.

Los datos a registrar y mantener se detallan en 3.2.3 Mantenimiento de UAS.

3.1.6 Datos de los Observadores.

En este bloque se registra la información relativa a los Observadores, mediante datos como los siguientes:

- Tipo y número de documento. En el modo alta, el tipo y el número de documento se contrastará contra la tabla pilotos, ya que los observadores suelen ser pilotos también, para cargar los datos del piloto como observador.
- Nombre y apellidos.
- Fecha nacimiento.
- Teléfono y Correo Electrónico.

3.1.7 Documentación.

En este bloque se registran los archivos relativos a las comunicaciones no tipificados ya en la aplicación, como: certificaciones, pólizas, la propia solicitud cuando la comunicación viene de sede electrónica, los correos electrónicos para subsanaciones, etc.

3.1.8 Valoraciones de la UVR, JOCI y GT.

En este bloque se registran y mantienen los datos propios de las valoraciones de la UVR, JOCI y GT. La información a recoger será del tipo:

- La Valoración podrá ser: “Pendiente”, “Positiva” y “Negativa”.
- Agente que realiza la valoración.
- Observaciones: información relativa a la valoración de la unidad.
- Documentación: apartado para incluir documentación asociada a la valoración de la unidad, se podrán adjuntar varios documentos.

3.1.9 Valoraciones de las Comisarías.

En este bloque se registran y mantienen los datos propios de las valoraciones de las comisarias implicadas como:

- La Valoración podrá ser: “Pendiente”, “Positiva” y “Negativa”.
- Comisaría: inicialmente será la que corresponda según la demarcación del punto de partida del vuelo. Pudiendo entrar a valorar otras comisarías en un nuevo bloque de valoración porque la Territorial en base a la zona de vuelo lo considere.
- Agente que realiza la valoración.
- Observaciones: información relativa a la valoración de la unidad.
- Documentación: apartado para incluir documentación asociada a la valoración de la unidad, se podrán adjuntar varios documentos.

3.1.10 Búsqueda de Comunicaciones

Se podrán consultar las comunicaciones que ya se encuentran dadas de alta en el sistema por cualquiera de los criterios de búsqueda propuestos. Estos filtros de búsqueda podrán ser:

- Relativos a la Comunicación, como:

  - Número de Comunicación, Referencia Tramitagune o Referencia del Ministerio.
  - Fecha desde/hasta del registro de la comunicación
  - Sede Electrónica: Si/No. Filtro para poder filtrar las comunicaciones que llegan desde Sede Electrónica, las que llegan por otra vía o ambas.
  - Estado comunicación: En proceso o Finalizada.
  - Valoración de Comisarías: para poder filtrar por la valoración de las Comisarías a la operación (Pendiente, Positiva, Negativa). Como una misma operación puede tener valoración de varias Comisarías, con que una sola valoración haya sido negativa, se considera que la valoración de Comisarías es negativa. Por lo tanto, si se selecciona “Pendiente” y/o “Positiva”, si alguna valoración de las Comisarías es negativa dicha comunicación no aparecerá en el resultado de la búsqueda. En caso contrario aparecerán aquellas comunicaciones que tengan alguna valoración “Pendiente” y/o “Positiva”. Si se selecciona “Positiva” en el combo y no hay ninguna valoración negativa y hay una positiva para una comunicación, se mostrará, aunque pudiera tener también valoraciones pendientes.
  - Valoraciones de JPOPI, UVR u JOCI.

- Relativos a la Operadora, como:
  - Tipo de Documento de la entidad operadora, los tipos de documentos serán CIF, DNI, NIE, Pasaporte, otros.
  - Número de documento de la entidad operadora.
  - Razón Social / Nombre Apellidos: Razón Social o Nombre y Apellidos de la operadora.
  - Código Referencia AESA: el código emitido por AESA para la operadora.
- Relativos al Piloto, como:
  - Tipo de documento identificativo del piloto, los tipos de documentos serán DNI, NIE y Pasaporte.
  - Número de documento identificativo del piloto.
  - Nombre y apellidos del piloto.
- Relativos a la Operación, como:
  - Tipo de operación del vuelo.
  - Categoría de operación de vuelo.
  - Fecha de inicio desde/hasta del vuelo
  - Fecha de fin desde/hasta del vuelo
  - Territorio Histórico del lugar del vuelo.
  - Municipio del lugar del vuelo.
  - Clase de UAS utilizada

Tras la búsqueda, en la tabla de resultados se podrá geoposicionar la información, mostrando en la cartografía corporativa los lugares donde volarán los drones de aquellas comunicaciones que cumplen con los criterios de búsqueda introducidos. Se utilizará el visor GisBisorea con toda la funcionalidad que la herramienta ofrece (activación de capas, medidas, dibujos, exportaciones).

Para cada registro de la tabla de resultados se podrá avanzar a la información de detalle.

3.2. Mantenimiento de Datos Maestros.

Este módulo facilita el registro y mantenimiento de las tablas maestras de Operadoras, Pilotos y UAS de la aplicación.

3.2.1 Mantenimiento de Operadoras.

Este módulo permitirá registrar y mantener los datos relativos a las Operadoras, mediante la operatoria habitual de búsqueda, lista y detalle. La información que se recogerá de las Operadoras es, como mínimo:

- Tipo y Número documento.
- Código de referencia AESA: código que proporciona AESA a la Operadora.
- Razón Social/Nombre y Apellidos.
- Domicilio/Sede Social.
- Seguro y Fecha de validez.
- Datos de contacto: teléfono y correo electrónico.
- Póliza de Responsabilidad, fecha de validez de la póliza y documento de la póliza.

3.2.2 Mantenimiento de Pilotos.

Este módulo permitirá registrar y mantener los datos relativos a los Pilotos, mediante la operatoria habitual de búsqueda, lista y detalle. La información que se recogerá de los Pilotos será del tipo:

- Tipo y número de documento, nombre y apellidos, fecha de nacimiento, sexo, nacionalidad.
- Domicilio.
- Teléfono y correo electrónico.
- Competencias teórico-prácticas. Indicando las capacitaciones adquiridas: A1-A3, A2, Autopráctica, STS01, STS02, Radiofonista, Otros a especificar.

3.2.3 Mantenimiento de UAS.

Este módulo permitirá registrar y mantener los datos relativos a los UAS, mediante la operatoria habitual de búsqueda, lista y detalle. La información que se recogerá de los UAS será, al menos:

- Clase de UAS, Número de controladora de vuelo, Marca y modelo, Nº Serie, MTOM y DRI (Sistema de identificación a distancia directa).

3.3. Zonas restringidas.

Este módulo permitirá registrar y mantener los datos relativos a las zonas restringidas para vuelos, por infraestructuras sensibles u otras causas, delimitando estas zonas con ayuda del visor cartográfico y mediante la operatoria habitual de búsqueda, lista y detalle.

3.4. Área de Análisis de Comunicaciones de Vuelos de UAS.

La nueva aplicación Gestión de Comunicación de vuelos de UAS deberá disponer de un subsistema de consulta de datos estadísticos. El subsistema deberá permitir acotar la información estadística a mostrar por:

- Operadora
- Piloto
- Valoraciones
- Ubicación
- …

La solución planteada deberá integrarse dentro del sistema de inteligencia empresarial corporativo, mostrando la información mediante Cuadros de Mando y/o documentos interactivos, de interfaz visual, gráfica y de manejo fácil e intuitivo.

Las tareas a realizar consistirán en:

- Implementar los procesos ETL para almacenar la información que actualmente no está recogida en el repositorio de datos del sistema de inteligencia empresarial.
- Creación de un informe interactivo para obtener información ad-hoc
- Creación de un cuadro de mando dinámico
- Embeber estos informes dentro de la aplicación mediante REST API

3.5. Integración con el sistema de gestión incidental

La información de los vuelos que se van a llevar a cabo se trasladará al sistema de gestión incidental para planificar la correspondiente actuación.

3.6. Consideraciones adicionales

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 eficiencia de los sistemas aprovechando los 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. Proteger el sistema de posibles indisponibilidades y/o alertar en caso de que se produzcan

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 DGTSI.
- **Servicios:**
  La nueva aplicación de portal se integrará con los servicios horizontales definidos según necesidades del análisis (gestor documental, Segurdok, concurrencia, auditoría, NORA, cartografía, correo…)
- **Usabilidad:**
  La nueva aplicación de portal deberá seguir la guía de estilos que se proporcione por la DGTSI.
- **Navegadores**
  Se deberá garantizar que sea accesibles desde el navegador 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 la intranet corporativa y proveerá de los servicios necesarios para resolver las peticiones y respuestas a las aplicaciones.

3.6.1 Calidad y seguridad del código entregado

El código entregado como resultado del proyecto deberá cumplir tanto los requisitos de arquitectura como las normativas de desarrollo que establezca el DSGV, así como superar los umbrales de calidad y seguridad establecidos, que están definidos por:

- Herramientas de análisis estático de código
- Auditorías en las que se podrá realizar una inspección y revisión manual del código.

3.6.2 Cobertura en pruebas automatizadas

Las pruebas automatizadas de las aplicaciones son una parte fundamental del proyecto para la garantía de calidad.

Los entregables deberán incluir al menos un conjunto de pruebas unitarias y de integración con un porcentaje de cobertura respecto al código creado que, como referencia, nunca deberá ser menor del 50%.

Las pruebas se realizarán con las herramientas o librerías estándar como JUnit, Mockito y Arquillian.

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 y cuya presentación se implementa sobre el portal de la intranet corporativa.

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 de la intranet pueda ser accesible desde el navegador Microsoft Edge.

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 7.3 y Liferay DXP 7.3 o superior
- Desarrollo de EJBs sobre Oracle WebLogic Server 12.2.1.4

Desarrollo de Portlets y EJBs sobre Liferay y Weblogic

- Portlet 3.0 (JSR-362)
- Java Server Faces 2.2
- Primefaces 8.0 u 11.0
- EJB 3.2 + JPA 2.1
- OSGi R6 bundles
- Liferay MVC Portlet

Middleware de intercambio de información

- Oracle Service Bus 12c
- Mensajería IBM Websphere MQ 9.2

Automatización de Procesos

- Control-M
- Apache Ant
- Gradle

Gestión documental

- IBM DB2 Content Manager v8.5

Frameworks y estándares:

- Todos los desarrollos deben realizarse para la versión 8 u 11 de la JDK
- Framework GIDA.

- La DGTSI dispone de un conjunto de servicios horizontales y componentes reutilizables para dar solución a las necesidades comunes identificadas por las aplicaciones.

Servidor de Bases de datos

- DB2 z/OS v.12
- SQL Server 2019
- Oracle 12c

Repositorio de código fuente

- Azure DevOps Server 2020
- GIT

Repositorio Documental de Proyecto

- Microsoft SharePoint 2016.

Informes

- Herramienta de análisis de la información empresarial Microstrategy versión 2021, con especial funcionalidad en los módulos:
    - Developer
    - Microstrategy Web
    - Microstrategy Library
    - Embedding SDK
- Bases de Datos:
    - DB2 11.5 con Acelerador BLU
    - Ficheros planos
- Herramienta ETL: IBM InfoSphere DataStage es la 11.7.1.1

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 desarrollo y de soporte técnico.
- 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 y auditoría de calidad.
- 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 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, así como preparación de su despliegue en los entornos del Departamento de Seguridad.
- Llevarán a cabo las tareas de desarrollo y construcción de las funcionalidades necesarias para la gestión de las inspecciones oculares.
- 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.
- Realización de los test de calidad, así como solicitud de la auditoría de calidad al equipo de la DGTSI encargado de dicha tarea.

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. Además, se validará que se sigue la normativa y las pautas de generación de código establecidas.

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 DGTSI 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.
  - Manuales de uso, aplicados a los servicios, en caso de que se defina alguno
  - 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. Documentación no sexista

Toda la documentación, publicidad, imagen o material que se genere con motivo de la ejecución del contrato, la empresa o entidad adjudicataria deberá emplear un uso no sexista del lenguaje, evitar cualquier imagen discriminatoria de las mujeres o estereotipos sexistas y fomentar una imagen con valores de igualdad, presencia equilibrada, diversidad, corresponsabilidad y pluralidad de roles e identidades de género.

4.6. 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.

4.7. 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.

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 DSGV:

- No introducir software informático ajeno al DSGV.
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del DSGV, 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 DSGV 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 DSGV.
- 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 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, en lo relativo a lo que establece el RD 311/2022 de 3 de mayo.

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

2 Requisitos a cumplir para el desempeño en teletrabajo

Requisitos generales

- La política de seguridad establecida por defecto en el Departamento de Seguridad del Gobierno Vasco es **denegar cualquier tipo de acceso remoto**. Los intentos de conexión que se produzcan serán registrados.
- Los accesos remotos que se requieran deberán ser solicitados y autorizados.
- Las autorizaciones se realizarán por la Directora de Gestión de Telecomunicaciones y Sistemas Informáticos.
- Las conexiones remotas hacia *la infraestructura del Departamento de Seguridad del Gobierno Vasco* se establecerán **siempre** con carácter específico (a demanda) y con duración limitada al tiempo necesario para realizar las actividades para las que se produce dicha conexión.
- Todas las conexiones remotas entrantes serán registradas y pueden ser monitorizadas. Se registrarán los siguientes datos para auditorías:
    - Accesos fallidos y satisfactorios.
    - IPs origen desde las que se producen las conexiones.
    - Fechas y horas de los accesos.
- El Departamento de Seguridad se reserva el derecho a recabar en cualquier momento cualquiera de los equipos utilizados para acceso remoto para auditar el cumplimiento de los requisitos recogidos en el presente documento.

Requisitos de los equipos

Los equipos autorizados para el acceso remoto para teletrabajo cumplirán con los siguientes requisitos:

- Los equipos se utilizarán exclusivamente con fines laborales y para tal fin serán proporcionados por la empresa adjudicataria del contrato de servicios.
- Para el acceso a internet se utilizarán redes seguras, entendiéndose como seguras las redes que sean gestionadas por el usuario (red doméstica) o su empresa.
- Los equipos contarán con un lector de tarjetas digitales para la autenticación del usuario.

- Los equipos contarán con un dispositivo TPM2.0.
- El sistema operativo será Microsoft Windows, en versiones soportadas y con licencia oficial de Windows 10 o superior.
- Los discos locales estarán cifrados con BitLocker.
- Se aplicarán las actualizaciones recomendadas por el fabricante del sistema operativo con una periodicidad no superior a 60 días.
- El equipo tendrá instalado y operativo un software EPP o EDR actualizado diariamente.
- Se remitirá por cada equipo un listado del software adicional instalado, incluyendo versiones, para su autorización expresa por el Departamento de Seguridad.
- La BIOS del dispositivo estará protegida por una contraseña robusta.

Requisitos de los usuarios

Los usuarios autorizados para el acceso remoto para teletrabajo cumplirán con los siguientes requisitos:

- Estarán dados de alta en el Directorio Activo del Departamento de Seguridad.
- Utilizarán la conexión al Departamento de Seguridad exclusivamente con fines laborales.
- El usuario deberá desconectar las sesiones de VPN una vez haya finalizado su trabajo no estando permitido en ninguna circunstancia dejar abiertas las conexiones fuera de la jornada laboral.
- Notificará cualquier deficiencia en el funcionamiento de los sistemas al servicio Arreta, en especial si consideran que pueden estar siendo víctimas de un ciberataque. En este caso se abstendrán de utilizar el acceso remoto hasta que la situación haya sido revisada y tener la autorización pertinente.
- Utilizará en el equipo local, cuando vaya a realizar una conexión a la infraestructura del Departamento de Seguridad, un usuario sin permisos de Administrador Local.
- El usuario firmará el documento NS04-A aceptando las Normas de Seguridad para colaboradores y el documento NS10 del "Régimen de trabajo fuera de los locales del Departamento de Seguridad".
- Adicionalmente firmará una copia de este documento asumiendo los requisitos que en él figuran.

3 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.