Nuevo Sistema de Información Schengen

SIS RECAST

Pliego Prescripciones Técnicas

Contenido

1. INTRODUCCIÓN 4

2. OBJETO DEL CONTRATO 4

3. ALCANCE 5

3.1. ANTECEDENTES SIS 5

3.2. DESCRIPCIÓN DEL SISTEMA 6

3.2.1 ACTUALIZACIONES 9

3.2.2 DATOS BIOMÉTRICOS/IMÁGENES 10

3.2.3 CONSULTAS 11

3.2.4 CONSISTENCIA 11

3.2.5 NOTIFICACIONES (COMUNICACIONES POLICIALES UNIDIRECCIONALES) 12

3.2.6 ERRORES 13

3.2.7 RELACIONES 13

3.2.8 CONSULTA DE PIZARRAS 13

3.2.9 INTERFACE SIP 13

3.2.10 AVISOS 14

3.2.11 ESTADÍSTICAS E INFORMES 14

3.2.12 MENSAJERÍA 15

3.3. CARACTERÍSTICAS 16

3.4. SEGURIDAD DE ACCESO 16

3.5. AUDITORIA 17

4. METODOLOGÍA APLICABLE Y ENTORNO TECNOLÓGICO 17

5. ENTREGABLES 19

6. PLANIFICACIÓN Y ORGANIZACIÓN 19

6.1 MECANISMOS DE SEGUIMIENTO Y CONTROL 19

7. PLAN DE ENTREGAS E HITOS DE CONTROL 20

8. CONFIDENCIALIDAD, SEGURIDAD Y PROP. INTELECTUAL 20

8.1 ACCESO Y PROTECCIÓN DE DATOS 20

8.2 NORMAS DE SEGURIDAD RELATIVAS A LOS S.I 21

8.3 PROPIEDAD INTELECTUAL 22

9. GESTIÓN DE LA CALIDAD 22

10. GESTIÓN Y ADMINISTRACIÓN DEL SERVICIO 24

11. LUGAR DE EJECUCIÓN DEL CONTRATO 24

1. INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información del Gobierno Vasco establece una política de seguridad centrada en los servicios propios de la Administración electrónica, por ello, dada la singularidad y especificidad que presenta el ámbito de la seguridad pública, se aprueba dentro del Departamento de Seguridad la *"Orden de 23 de enero de 2019, de la Consejera de Seguridad, por la que se aprueba la Política de Seguridad de la Información en el ámbito de las redes y servicios de información gestionados por el Departamento de Seguridad"* y es el propio Departamento de Seguridad el responsable de la planificación y mantenimiento de redes de comunicación y sistemas de información en el ámbito de la seguridad pública. Dicha orden, contempla la estructura organizativa que instrumenta la Política de Seguridad de la Información y será Responsable de la Seguridad y de los Sistemas, la Dirección de Telecomunicaciones y Sistemas de Información, sin perjuicio de las atribuciones que correspondan a otros en el ámbito propio del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco.

Por tanto, 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).

La DGTSI, en el desarrollo de los sucesivos planes de Gestión de Sistemas en continua evolución, aborda una serie de proyectos que actualizan y mejoran los sistemas de información que pone a disposición de sus clientes y usuarios. Tal y como se detalla en el presente documento, el objeto del contrato está enmarcado en actividades propias dentro del ámbito de la seguridad pública integrado con el Sistema de Información Policial de la Ertzaintza (SIP).

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. OBJETO DEL CONTRATO

El objeto del presente expediente es la Contratación de los servicios para realizar las tareas de definición, diseño, construcción e implantación de un aplicativo que:

- gestione y efectúe las actualizaciones y consultas al nuevo Sistema de Información Schengen RECAST, evolución del actual SIS II, según las nuevas funcionalidades establecidas por SIS RECAST y adaptándose al nuevo diseño de BDSN (Base de datos de señalamientos nacionales),
- garantice la rapidez y calidad de la información, así como la integración de todos sus datos con el aplicativo de SIP (Sistema de Información Policial).

En el momento de la adjudicación del contrato, se aplicará la última versión disponible de la documentación, y se tendrán en cuenta todas las modificaciones posteriores que pudieran producirse durante los trabajos de desarrollo, tanto en lo referente a la comunicación con el sistema central como a la integración con el SIP de Ertzaintza.

En la actualidad, Ertzaintza tiene disponibles todas las funcionalidades que SIS II pone a disposición de los cuerpos de seguridad. Sin embargo, debido al nuevo marco normativo que regula el Sistema de Información Schegen y la importancia y calado de las modificaciones necesarias para la adaptación del sistema actual, tanto desde el punto de vista de categorías a considerar, los datos incorporados como los flujos y lógica

de negocio, se hace necesario el desarrollo de un sistema nuevo para cumplir con las obligaciones derivadas de los Reglamentos Europeos.

El nuevo aplicativo, además de realizar actualizaciones y consultas a SIS RECAST, a grandes rasgos se encargará de desarrollar:

- funcionalidades compartidas con el sistema central como son la consistencia y notificaciones,
- funcionalidades propias del aplicativo para facilitar la labor del operador Schengen: alertas, procesos background, envíos automáticos y manuales...
- otras funcionalidades para comprobar y mantener la coherencia de información en SIP: relaciones, informes periódicos y aperiódicos, estadísticas, control de datos vigentes y otras cuestiones de interés.

Todo ello sin olvidar, por una parte, la labor de traslacción/creación de codificaciones vigentes o nuevas en SIP, en base a la codificación que se reciba del sistema central (tanto codificación nacional como codificación SIS), y por otra parte, la seguridad a implementar, tanto para el aplicativo propio (según normativa del departamento de Seguridad), como para la concordancia que sea necesaria con la normativa de seguridad que implante el sistema central nacional.

Se realizarán asimismo las correspondientes modificaciones en el actual sistema de información policial (SIP) de la Ertzaintza, en todos los puntos en los que actualmente se solicita información a SIS, para adecuarse tanto a los nuevos formatos de llamadas y respuestas como a la nueva información disponible, y también en nuevos puntos que surgirán como consecuencia de las nuevas categorías/funcionalidades que incluye el sistema central.

Todo ello implica una relación estrecha entre el nuevo aplicativo de comunicación con SIS RECAST y el sistema de información policial (SIP) de la Ertzaintza.

3. ALCANCE

3.1. Antecedentes SIS

El Sistema de Información de Schengen (SIS) constituye un instrumento esencial para la aplicación de las disposiciones del acervo de Schengen integrado en el marco de la Unión Europea. Este sistema almacena alertas sobre personas y objetos en relación con el control del espacio Schengen, con la finalidad de garantizar la seguridad en dicho entorno. Actualmente se está utilizando el Sistema de Información Schengen de segunda generación (SIS II), basado en:

- un Sistema Central (CS) ubicado en Estrasburgo (Francia) que soporta la Base de Datos Schengen (CS-SIS)
- Sistemas Nacionales que gestionan una serie de operaciones relativas a determinadas categorías en una base de datos replicada, denominada "Sistema Nacional SIS" (NS.SIS), que recibe las peticiones de las Oficinas de Enlace SIS (OE.SIS) y las cuales a su vez reciben las peticiones de las distintas Fuerzas y Cuerpos de Seguridad del Estado a través de sus respectivos HOSTs, sistemas propietarios de cada Organismo.

Técnicamente la comunicación entre el sistema de información policial de la Ertzaintza y el sistema central (NS.SIS) se realiza vía servicios web. Actualmente Ertzaintza

consulta y alimenta el sistema SIS II (datos alfanuméricos, anexos e información biométrica), consumiendo los SW que el sistema central expone para esos fines. El servicio a invocar en cada caso depende de la información origen (lo que se denomina categoría: personas, vehículos, armas...), de las posibles relaciones que se puedan generar (interlinks) y de la acción a realizar (lo que se denomina operación: alta, modificación, cese, consulta...). Asimismo se garantiza tanto la calidad como la coherencia de la información actualizada por medio de otros procesos compartidos tales como consistencia y notificaciones (además de interlinks), y todos los datos se integran con SIP por medio de relaciones y explotaciones de datos.

Toda la información enviada a SIS se almacena en el SIP de Ertzaintza en unas bases de datos intermedias denominadas "pizarras", que constituyen una réplica de la información que desde Ertzaintza se envía al sistema central, en el formato SIS.

Este esquema de integración, actualmente en uso con SIS II, seguirá siendo el mismo para el nuevo aplicativo de comunicación con SIS RECAST: SW para comunicación con el sistema central y almacenamiento de la información enviada en BBDD propias (pizarras). Además, el nuevo aplicativo deberá cumplir los requisitos actuales, así como la comunicación de nuevas categorías y toda la normativa que el sistema SIS RECAST determine.

3.2. Descripción del sistema

A continuación se resumen los requisitos funcionales en base a la documentación disponible a la fecha.

Las funcionalidades citadas en este documento deberán ser detalladas y ampliadas por el contratista en la fase de toma de requisitos del sistema, obteniendo como resultado un catálogo de requisitos que contemplará toda la funcionalidad del nuevo sistema, y que requerirá la aprobación formal de la DGTSI antes del inicio de los trabajos de análisis y desarrollo del sistema.

En la toma de requisitos se ha de incluir todas las funcionalidades de la aplicación SIS II (actualmente en operación), además de la aportada por SIS RECAST.

Los principales cambios de SIS RECAST respecto a SIS II serían la generación de nuevas categorías y la ampliación de información de las existentes, nuevas consultas, relaciones entre categorías, la generación de nuevas operaciones de los SW y la remodelación del sistema de seguridad y auditoría, entre otros.

Actualmente, SIS II contempla las siguientes categorías:

- Personas buscadas (desaparecidas/requisitoriadas)
  - Víctimas de identidad usurpada
  - Víctimas de malos tratos
  - Domicilios de malos tratos
- Vehículos (completo, documentación, placas)
- Objetos
  - Armas de fuego
  - Documentos en blanco
  - Documentos expedidos

- Documentos oficiales: esta categoría pasa a denominarse "Medios de pago monetarios"
- Billetes de banco
- Aeronaves
- Embarcaciones
- Motores de embarcaciones
- Equipamiento industrial
- Contenedores
- Objetos numerados
- Obras de arte

Estas categorías amplían su contenido con nuevos campos, y también amplían/cambian su funcionalidad. A éstas, se añaden las siguientes nuevas categorías creadas para SIS RECAST:

- Motores de aeronaves: se incluye como categoría nueva y como entidad dependiente de la categoría de aeronaves.
- Artículo de tecnología de información
- Parte de vehículo
- Parte de equipamiento industrial: se incluye como categoría nueva y como entidad dependiente de la categoría de equipamiento industrial.
- Objetos de gran valor

Esta modificación y ampliación supone varios requisitos: por una parte, el intercambio de datos deberá estar adaptado a la interacción con el sistema central nacional (que a su vez, estará adaptado al sistema europeo). Por otra parte, teniendo en cuenta que los datos a enviar siempre tienen su origen en SIP, esto implica directamente cambios en SIP: ampliación de información en la recogida de datos y/o cambio de condiciones (obligatoriedad, cambios de formato, traslaciones, etc.), con todo lo que ello deriva: cambios de textos de diligencias, etc., además de la realización de más validaciones previas al envío a BDSN, adaptándose a la normativa.

Respecto a las funcionalidades compartidas con SIS RECAST, automáticas o solicitadas por el operador Schengen, se consolidarán consumiendo los SW que el sistema central expone en cada caso, en su mayoría, síncronos. Se realizarán los envíos oportunos al sistema central, manteniendo en todo momento la integridad con el sistema policial propio de Ertzaintza.

Para todas las categorías (existentes y nuevas), en el nuevo aplicativo, y únicamente en lo referente a la gestión compartida con el sistema central, deberá realizarse:

- SW de intercambio de información: alta, cese, modificación y consulta, y cualquier otra funcionalidad que el sistema central exponga, incluyendo información alfanumérica, anexos, información biométrica, ADN, según categoría, todo ello en base a la normativa SIS (consultas previas, etc.).
- Operaciones necesarias para cada servicio de intercambio: consultas variadas, modificaciones parciales, relaciones, etc...
- Validaciones sintácticas y funcionales antes de cualquier operación, interna o externa.

- Actualización de información en las "pizarras" de Ertzaintza en base a los datos enviados a SIS RECAST, o en base a actualizaciones realizadas por otros cuerpos en alertas compartidas (recepciones).
- Grabación de registros de auditoría.

Y en SIP:

- Cambios y ampliación de datos de recogida de información: pantallas, BBDD (origen y pizarras), textos de diligencias...
- Modificaciones en las llamadas a SW, posibles altas automáticas, chequeos, procesos background...
- Aumento de las validaciones sintácticas y funcionales antes de consolidar cualquier operación, interna o externa.
- Almacenamiento/borrado de información en las "pizarras" de Ertzaintza en base a los datos recogidos en SIP.
- Grabación de registros de auditoría.

Añadiendo a todo esto la gestión propia de la información.

La ampliación/remodelación de las categorías supone que los servicios generales de consistencia Nacional y notificaciones nacionales se deberán adaptar a las nuevas características.

Todas las categorías, existentes y nuevas, podrán incluir anexos.

Respecto a personas buscadas, por ejemplo, se añaden nuevas categorizaciones como son órdenes de expulsión, decisiones de retorno, personas vulnerables, etc. Se amplía la información de las personas incluyendo documentos con sus imágenes, números de registro, etc..

Las huellas de personas buscadas cambian en formato y tamaño (sin límite). Sobre este tipo de información, cabe resaltar que SIS RECAST incluye también el intercambio de huellas latentes (personas desconocidas). En ambos casos, deberá realizarse la comunicación directa del nuevo aplicativo con el sistema MorphoBis (identificación biométrica) para extracción del archivo NIST en formato SIS, así como la generación de los avisos que operativamente se consideren necesarios sobre estos intercambios, manteniendo la integridad de los datos enviados con MorphoBis en todo momento.

También se incluye el intercambio de ADN de personas, asegurando el estándar CODIS. Este intercambio previsiblemente se realizará vía manual.

El nuevo Sistema ofrece la posibilidad de asociar alertas de diferentes categorías, como puede ser la asociación de personas a objetos. Esto supone la creación de todas estas categorías como entidades dependientes de la categoría origen, dato a tener en cuenta en las pizarras y BBDD de Ertzaintza. El Sistema Central será el que determine qué categorías se pueden asociar. En el caso de personas, se podrán asociar a los siguientes objetos como mínimo:

- ☐ Vehículos
- ☐ Embarcaciones
- ☐ Embarcaciones con sus motores
- ☐ Contenedores
- ☐ Aeronaves
- ☐ Aeronaves con sus motores
- ☐ Armas de fuego

□ Documentos en blanco

En el sistema central se tendrá en cuenta, tanto a nivel de consultas como de ceses de una entidad, todas sus extensiones, ofreciendo operaciones específicas para obtener/actualizar toda la información en llamadas únicas (para cualquier categoría que admita ésta operativa). Este "efecto dominó" se debe tener en cuenta a la hora de las actualizaciones de las pizarras y auditorías propias de Ertzaintza, así como a la hora de recoger y visualizar los datos que se devuelven en las consultas (navegación). Toda esta casuística completa tendrá el mismo funcionamiento para todas las posibles relaciones que se generen en el sistema central nacional (links).

Sobre estas casuísticas, tener en cuenta que al sistema central nacional llegarán mensajes de difusión, mensajes que podrá recibir Ertzaintza en forma notificaciones, u otra vía.

Los actuales procesos programados deberán adaptarse a las características del nuevo sistema, y se realizarán nuevos procesos si operativamente se consideran necesarios, por ejemplo, el tratamiento específico para OEDE's.

Todas las pantallas multilínea del aplicativo ofrecerán la posibilidad de reordenación por cualquier columna.

3.2.1 Actualizaciones

La Ertzaintza, así como el resto de Fuerzas y cuerpos de seguridad del Estado, deberá alimentar dicho sistema tal como lo viene haciendo con el actual SIS II, en base a determinada información y referencias policiales que los usuarios introducen en el SIP. Esta información se almacenará desde SIP en bases de datos "pizarras" que la nueva aplicación visualizará y gestionará para integrar los datos adecuadamente en SIS RECAST. Estas "pizarras" son el punto intermedio entre SIP y SIS RECAST: se cargan/actualizan desde SIP y se actualizan (vigencias, ceses, notificaciones...) desde SIS RECAST. Los operadores Schengen, deberán poder validar la información que llega a sus pizarras, y proceder a la actualización de datos en el sistema central tal como marca la normativa (consultas previas, validaciones...). En determinadas circunstancias en las que los hechos están plenamente tasados, esta comunicación se realiza de forma directa sin que el operador Schengen necesite dar su "visto bueno", realizando la consulta previa en background (siempre que las codificaciones propias y centrales tengan correspondencia 1-1 y la normativa lo permita), generando notificaciones (comunicaciones policiales unidireccionales), del automatismo realizado.

Cada vez que entra información en las pizarras, el aplicativo activará avisos (por el método que se estime más operativo) para que el operador sea conocedor de la existencia de datos para comunicar, con especial énfasis en el caso de OEDEs.

El intercambio de información incluye tanto datos alfanuméricos como imágenes (formatos admitidos por SIS RECAST) que se encuentren relacionadas con cada uno de estos hechos, así como datos biométricos (MorphoBis) de las personas que se comuniquen, si se disponen de ellos, y ADN (LIMS). Las huellas enviadas deben cumplir el estándar NIST establecido por EuLISA. En cuanto a perfiles de ADN, será un binario asociado a la persona que cumplirá el estándar CODIS.

Antes de cualquier envío el operador deberá visualizar toda la información a enviar, tanto alfanumérica como imágenes, biométrica, etc. (salvo envíos automáticos en su caso). Una vez confirmado que desea hacer el envío, la aplicación comprobará que la

información cumple la normativa SIS, tanto sintáctica como funcionalmente, no permitiendo el envío en caso contrario, informando al operador detalladamente. Después de cualquier envío, mostrar al operador tanto errores como todas las advertencias recibidas, almacenando esta información para poder proceder a la subsanación. La operativa con las advertencias dependerá del calado de la relación de advertencias que envíe el sistema central.

Toda información enviada a SIS RECAST se almacenará en la pizarra correspondiente, y estos datos serán consultables por los operadores.

Estas actualizaciones provendrán siempre del SIP, mediante las referencias definidas para ello, es decir, todo lo que se envíe a SIS debe tener reflejo en SIP, y estar en la misma situación operativa/administrativa. Las referencias policiales que alimentarán SIS RECAST estarán previamente tasadas, y básicamente corresponden con requisitorias judiciales (determinados tipos de oficio), denuncias asociadas a personas desaparecidas, denuncias sobre robos, sustracciones, perdidas de objetos o buscados a efectos de pruebas en procedimientos penales, vehículos o parte de ellos, víctimas de malos tratos y sus domicilios, etc. y los posibles objetos implicados en ellas. En definitiva, todo lo relacionado con las actuales categorías y las nuevas, en materia de seguridad.

Además, se podrán realizar interlinks entre señalamientos y/o identidades. Esta herramienta genera relaciones entre datos enviados, relaciones que se envían y reflejan en el sistema central, todo ello siguiendo la normativa SIS RECAST, y que también deberán almacenarse en SIP.

Los señalamientos a enviar a SIS que estén previamente generados por otros cuerpos se gestionarán de forma que no generen duplicidades en el sistema central (relaciones internas, por ejemplo), ofreciendo al operador esta funcionalidad desde el aplicativo. Será necesario mantener estas relaciones "al día" según actualizaciones realizadas en el sistema central, por medio de procesos periódicos contra la BBDD del sistema central.

Desde Ertzaintza no se soportan identidades usurpadas, por lo que en este momento está operación no se contempla en las actualizaciones, pero sí las consultas.

En actualizaciones, los códigos propios de Ertzaintza compartidos con SIS deberán tener su correspondiente equivalencia con la codificación central, tanto nacional como internacional, ya que en las actualizaciones la codificación a enviar siempre será la centralizada, a un ámbito u otro, según indique la normativa.

3.2.2 Datos biométricos/imágenes

Actualmente, todas las imágenes a enviar a SIS previamente se cargan en SIP, se almacenan en el contenedor de documentos, y se genera el correspondiente apunte en las BD pizarra. La aplicación trata estos apuntes de pizarra de la misma forma que los apuntes de datos alfanuméricos.

En el caso de imágenes de personas y huellas, la nueva aplicación deberá disponer de la funcionalidad de enviar dichas huellas tanto por el sistema indicado (pizarra) como obteniendo la información automáticamente del sistema de identificación biométrica MorphoBis, por medio del consumo de SW propios de la herramienta, al igual que en el caso de ADN.

La nueva aplicación deberá permitir la previsualización de archivos a enviar, así como mostrar los archivos recibidos en las consultas realizadas por los usuarios, en todos

los formatos admitidos por SIS, entre los que destacamos JPG, NIST, PDF. A modo orientativo, los formatos admitidos en la actualidad (SIS II) son los siguientes:

DOC (Microsoft Word)
CSV (Comma Separated Values)
XLS (Microsoft Excel Spreadsheet
MPEG (Movinf Picture Experts)
JPEG (Joint Photography Expert Group)
GIF (Graphics Interchange Format)
TIFF (Tagged Image File format)
PNG (Portable Network Graphic)
BMP (Bitmap)
PDF (Portable Document Format)
NIST (Sirpit)

La nueva aplicación se basará en la relación de formatos admitidos por SIS RECAST, en los que se incluirá el formato en el que se intercambie la información de ADN.

En el caso de consultas, las imágenes ofrecidas por el sistema deben poder descargarse y/o enviarse a otras secciones de Ertzaintza para su estudio.

3.2.3 Consultas

La información que todos los Cuerpos y Fuerzas de Seguridad proporcionan al SIS RECAST estará disponible para consulta por todos y cada uno de ellos, en el formato preestablecido por el sistema. Se diseñarán y realizarán todas las operaciones de todas las categorías que el sistema central exponga y que resulten de interés al operativo de la Ertzaintza.

En base a la categoría a consultar, se invocará el SW correspondiente en función de la necesidad, permitiendo en los casos posibles la navegabilidad entre categorías relacionadas.

Asimismo, se realizarán las consultas denominadas "multicategorías", consultas que se realizan simultáneamente sobre varias categorías y que el sistema central expone, sin necesidad de invocar varios SW. Entre ellas, consultas de personas/objetos, consultas de transponders (para todos las categorías que lo informan), o por número de serie o registro.

Toda la información recibida en todos los casos se mostrará al operador tal como viene del sistema central, mostrando claramente las relaciones generadas y permitiendo la navegabilidad. Esto incluye la codificación, que se mostrará según la envíe el sistema central.

3.2.4 Consistencia

La aplicación deberá disponer de los desarrollos para permitir solicitar consistencia nacional de datos al sistema central como para recibir las solicitudes de consistencia procedentes del sistema central, todo ello a modo de control de calidad de la información entre ambos sistemas.

El proceso de solicitud y recepción de esta funcionalidad se adaptará a la normativa de SIS RECAST, incluyendo las nuevas categorías y datos. En líneas generales:

1. Cuando la comparación la solicite el Sistema central, se hará mediante un proceso en background, emitiendo respuesta al solicitante.
2. La comparación solicitada desde el sistema de la Ertzaintza se realizará de forma periódica, será un proceso planificado (en background). No obstante, en este caso se dotará al operador la posibilidad de solicitar consistencia de determinados señalamientos, con respuesta síncrona, bien desde la consulta de pizarras, bien desde otros puntos del aplicativo.

Los resultados de la consistencia en cualquiera de los sentidos se podrán consultar por el aplicativo, y se ofrecerá la posibilidad de subsanar la inconsistencia.

Las deficiencias encontradas por este contraste será responsabilidad de los operadores el subsanarlas, marcando la corrección. Se activarán avisos para indicar al operador que hay diferencias pendientes de subsanar, mostrándolas en pantalla, estableciendo medidas para la subsanación de los errores detectados, modificando la pizarra réplica y las bases de datos que se consideren necesarias.

Estos procesos también guardan auditoría.

3.2.5 Notificaciones (comunicaciones policiales unidireccionales)

Todas las notificaciones recibidas podrán consultarse por medio de este nuevo aplicativo, según criterios de selección en función del tipo de notificación. Adicionalmente, determinadas notificaciones recibidas, a criterio operativo, mostrarán un aviso que informe de la existencia de notificaciones "críticas" pendientes de visualizar, como pueden ser:

- Expiración del período de salida voluntaria en alertas de retorno
- Bajadas de ámbito
- Persona desconocida sin huella

Y cualquiera considerada crítica para el operativo.

En función de la notificación recibida, el sistema actualizará de modo automático la información de la/s pizarra/s correspondiente/s del sistema propio de Ertzaintza, así como las bases de datos afectadas por la notificación. Se indicará para cada una de ellas si se ha procedido a la actualización de datos propios de forma que se controlen este tipo de actuaciones. La consulta explícita de notificaciones mostrará también esta información.

El aplicativo mostrará tanto notificaciones externas (procedentes del sistema central), como notificaciones internas.

Adicionalmente, las modificaciones sobre datos origen de SIP, sobre todo en modo automático, pueden generar el envío automático de mail's al centro titular de la referencia SIP.

3.2.6 Errores

Toda comunicación con resultado erróneo o con advertencias se almacenará en bases de datos, y se podrá consultar on-line desde el aplicativo. El usuario debe ser conocedor de estas situaciones tanto errores como advertencias, en tiempo real, a fin de que las subsane en la medida de lo posible y necesario, pero también podrá consultar estas situaciones a tiempo pasado.

Para los señalamientos enviados al sistema central que dispongan de advertencias se activará la posibilidad de subsanar dichas advertencias, restaurando en estos casos esta base de datos de errores/advertencias.

3.2.7 Relaciones

Los señalamientos generados en SIS RECAST deberán tener su apunte correspondiente en el fichero de relaciones de SIP, de forma que al consultar información desde SIP podamos ver de forma inmediata los posibles apuntes en SIS RECAST sin necesidad de invocar los SW centrales. Estas relaciones, que deberán generarse (alta o borrado) de forma automática, permitirán la actualización manual en los casos que se necesite.

Por medio de relaciones se gestionarán los señalamientos duplicados con otros cuerpos, como se ha explicado anteriormente.

Todas las relaciones deberán mantenerse actualizadas. Los ceses de señalamientos de Ertzaintza llegarían por medio del servicio de notificaciones, pero las relaciones entre señalamientos, al no ser conocidas por el sistema central, se deben mantener actualizadas por medio de procesos internos.

3.2.8 Consulta de pizarras

El aplicativo ofrecerá la posibilidad de consultar los datos almacenados en las pizarras réplica, tanto datos vigentes como cesados. La consulta para cada categoría se podrá realizar por diversos datos (fechas vigor, expiración, ámbito, motivo/conducta, filiaciones, etc.), siempre según los formatos de intercambio (pizarras), aportando flexibilidad a las consultas que ofrece el sistema central.

Se podrán consultar también los intercambios de información biométrica, ADN o imágenes.

Por ejemplo, para todas las categorías, se podrá consultar por fechas de vigor, caducidad, motivo, conducta, referencial policial, señalamientos vigentes, ceses...

Para personas, además por datos filiación, fecha nacimiento. Para vehículos, por matricular o bastidor, marca, modelo. Otras categorías, por número de serie, etc...

3.2.9 Interface SIP

Desde numerosas opciones de SIP se invocan los SW de SIS RECAST para realizar chequeos u otras consultas. Todas estas opciones que tienen comunicación con SIS RECAST deberán modificar las llamadas a los SW para adecuar las consultas a los

nuevos formatos y respuestas recibidas, así como se podrán añadir las nuevas operaciones que se estimen oportunas, e incluso modificar alguna operativa en función de las consultas ofrecidas por el sistema central.

Como se ha indicado en el apartado "actualizaciones" de este pliego, toda información a enviar a SIS RECAST tiene su origen en el SIP. Esto implica que, por una parte, los cambios que se realicen en el sistema central sobre las categorías existentes deberán tener su correspondiente reflejo en nuestro sistema, y por otra, las nuevas categorías deberán implementarse, todo ello de cara a la recogida de información por parte de Ertzaintza, transferencia a las pizarras correspondientes y posterior envío a SIS RECAST: las categorías existentes se rediseñarán, las nuevas, se implementarán.

En definitiva, todos los nuevos conceptos que forman parte de SIS RECAST y se citan en este pliego, como personas desconocidas, partes de vehículo, etc., deberán tener su adaptación y correspondiente desarrollo en el sistema de información de la Ertzaintza. Esto implica nuevas validaciones, cambios de formato, recodificaciones, cambios de pantallas, bases de datos, textos de diligencias...

Actualmente, los SW se invocan desde diversos puntos: consultas únicas, chequeos de personas, consultas de movilidad, Datapol, chequeo de alojados, alquileres y joyas, Euskarri, visitas, policías locales....

La integración con SIP incluye la integración con el aplicativo de gestión de identidades UXUE, necesaria para el control de imágenes/huellas/otras identidades de la persona.

3.2.10 Avisos

Como se ha indicado, habrá situaciones que generen avisos en el aplicativo. En principio, estas situaciones serán:

- Existencia de actualizaciones en pizarras pendientes de enviar al sistema central
- Notificaciones "críticas" recibidas
- Datos inconsistentes sin resolver
- OEDEs pendientes
- Modificación de señalamientos propios/compartidos por otros cuerpos (ceses-notificaciones)
- Señalamientos vigentes propios con advertencias

La aplicación deberá estar preparada para mostrar avisos al operador de un modo flexible y dinámico.

3.2.11 Estadísticas e informes

El aplicativo ofrecerá la posibilidad de explotación estadística de datos vigentes, cesados, etc. para un periodo de fechas a elección del operador, con subtotales por categoría.

Los actuales informes intentan detectar situaciones indebidas entre nuestro sistema y lo enviado a SIS. Estos informes serían complementarios a la consistencia, a fin de aportar calidad a la información.

Los informes actuales a petición podrán ampliarse para adaptarse a las nuevas categorías. A día de hoy, por fecha desde-hasta, se dispone de los siguientes:

- Personas en SIP con más de una relación sobre dato insertado en SIS/BDSN y cuya numeración difiere en los 10 primeros números
- Personas de alta en SIS/BDSN con motivo control especifico, vigilancia discreta u orden detención policial, y reclamante no judicial
- Vehículos de alta en SIS/BDSN con motivo control especifico, vigilancia discreta, y órgano reclamante no judicial
- Personas con requisitoria abierta en SIP sin señalamiento SIS/BDSN procedente de Ertzaintza, que posean fecha nacimiento y nacionalidad
- Personas con requisitoria cerrada-cancelada en SIP, con señalamiento SIS/BDSN procedente de la Ertzaintza
- personas con ficha abierta como desaparecidas en SIP, sin señalamiento SIS/BDSN procedente de la Ertzaintza
- personas con ficha cerrada como desaparecidas en SIP, con señalamiento SIS/BDSN procedente de la Ertzaintza
- vehículos con ficha abierta como sustraído o similar en SIP, sin señalamiento SIS/BDSN procedente de la Ertzaintza
- vehículos con ficha cerrada como sustraído o similar en SIP, con señalamiento SIS/BDSN procedente de la Ertzaintza

Además de estos informes, es necesario poder obtener desde el nuevo aplicativo y con carácter mensual los datos operativos de altas y ceses por categoría que realiza la Ertzaintza, indicando el tiempo medio de generación y porcentaje correspondiente desde que entran en pizarra hasta que se envían a SIS RECAST, con las siguientes franjas horarias:

- menos de 4 horas
- entre 4 y 12 horas
- más de 12 horas

La información indicada en este apartado se obtendrá con Data Wharehouse, proporcionando el nuevo aplicativo un enlace directo sin necesidad de logearse de nuevo.

3.2.12 Mensajería

Se dispondrá de una funcionalidad para realizar comunicaciones internas/externas con objeto de agilizar las funciones que realizan los operadores Schengen. Se podrán realizar de forma automática las que previamente están definidas por el sistema, como pueden ser comunicaciones de aparición de persona extranjera, etc., quedando registradas todas estas comunicaciones.

Siempre que se cubran los requisitos, se hará uso de los servicios horizontales disponibles en DGTSI para esta funcionalidad.

3.3. Características

Teniendo en cuenta los objetivos estratégicos definidos y las funcionalidades que se van a proporcionar, es necesario que el aplicativo cuente con las características básicas siguientes:

- **Seguridad**:
  - ✓ Los servicios que se ofrecen podrán tener restringido su acceso en función del perfil del usuario que se conecte.
  - ✓ Se almacenará en el log de auditoría corporativo la información relativa a dicho acceso.
- **Multilingüismo:**
  - ✓ El nuevo aplicativo ha de contemplar la posibilidad de selección del idioma de navegación (Euskera o Castellano) por parte del usuario.
- **Accesibilidad:**
  - ✓ El aplicativo tratará de cumplir con los requerimientos legales establecidos al respecto.
- **Estadísticas y Monitorización:**
  - ✓ Él aplicativo permitirá realizar auditoria y monitorización de usuarios.
  - ✓ Se podrán realizar informes estadísticos de acceso.
- **Usabilidad:**
  - ✓ El aplicativo contará con formatos y estilos de los servicios unificados.
  - ✓ Se utilizará la guía de estilos definida por el departamento.

3.4. Seguridad de acceso

La oferta describirá las funcionalidades ligadas con los aspectos de seguridad de acceso y uso del sistema, indicando niveles de seguridad, gestión de perfiles, control de acceso a funcionalidades y datos, etc. Para ello, se deberán seguir las pautas y criterios establecidos por la DGTSI en su Plan de Seguridad relativo al desarrollo de aplicaciones J2EE.

A nivel de implementación de la aplicación, será el framework tecnológico de la DGTSI el que marcará la granularidad en el acceso a la información de cada uno de los roles de la aplicación (a nivel de pantalla, pestaña o campo).

Los usuarios con acceso al aplicativo dispondrán de un código de usuario para SIS unívocamente relacionado con el suyo, y siguiendo las especificaciones de seguridad del sistema central.

3.5. Auditoria

Se identificarán las funcionalidades asociadas a dejar rastro de las operaciones realizadas en el sistema, conforme a lo establecido en la LOPD y a la política de seguridad de la DGTSI indicando los movimientos a registrar así como la información asociada a cada uno de ellos.

Para ello, se utilizará el componente de auditoría en el framework de ejecución J2EE de la DGTSI.

Además, se deberán registrar, en el sistema de auditoría del SIP, todas las modificaciones realizadas por los operadores en tablas propias de SIP a través de esta nueva aplicación. Se grabarán los rastros de las modificaciones en las tablas disponibles al efecto, manteniendo los criterios aplicados en el resto de aplicaciones del SIP. Esta auditoría será consultable desde el aplicativo.

4. METODOLOGÍA APLICABLE Y ENTORNO TECNOLÓGICO

Deberán respetarse las convenciones y normativas adoptadas para desarrollo, funcionamiento y despliegue de aplicaciones recogidas en la normativa vigente.

En la realización y codificación de las unidades de tratamiento de las aplicaciones se utilizará una metodología estructurada y homogénea de diseño y programación, basada en incrementos o entregas parciales.

Las herramientas para el desarrollo deberán adecuarse a los estándares tecnológicos actualmente en vigor en la DGTSI.

La seguridad y control de acceso a las aplicaciones deberán utilizar el sistema de seguridad establecido como Administración de Usuarios y Seguridad para el Departamento de Seguridad.

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 J2EE hace referencia.

La arquitectura actual de ejecución de aplicaciones J2EE de la DGTSI, se basa en una Arquitectura Orientada a Servicios (SOA) sobre la que se ejecutan servicios J2EE sobre un framework de ejecución (Bidea) coreografiados desde flujos de negocio (procesos) y presentados en un aplicativo.

Entorno de desarrollo web:

- WebSphere Portal Server 8.5
- WebSphere Application Server 8.5
- Oracle Service Bus 12c
- IBM MQ 7.5
- Oracle RAC 12c

- DB2 z/OS v.11

Entorno de desarrollo host:

- Sistema Operativo IBM z/OS V2.3
- IBM WebSphere MQ Series V7.5
- IBM DB2 V11
- IBM CICS TS V5.5
- IBM VisualAGE Generator
- IBM Enterprise COBOL 4.2
- IBM TSO (JCL)
- IBM Personal Communications (Emulación 3270)
- IBM Office Vision Display Write 370 2.2
- IBM Image Plus 2
- IBM ASF 3.4

Informes:

- Herramienta de análisis de la información empresarial Microstrategy versión 10.11., con especial funcionalidad en:
    - Módulo Developer
    - Módulo Microstrategy Web
- Bases de Datos:
    - DB2 con Acelerador Blu
    - Ficheros planos
    - DB2 z/OS
- Herramienta ETL: IBM InfoSphere DataStage es la 11.3.1

Framework:

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

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.

5. ENTREGABLES

La realización de los desarrollos lleva implícitamente labores de análisis, programación y pruebas para una correcta implantación. Así mismo deberán tenerse en cuenta los impactos que puedan ocasionar los mantenimientos en otros sistemas y/o aplicaciones.

Durante las fases de análisis, diseño, desarrollo, pruebas e implantación la empresa adjudicataria deberá cumplimentar todos los documentos definidos como obligatorios dentro de la metodología y ciclo de vida definida por la DGTSI.

Para la realización de estas tareas se tendrán en cuenta las necesidades y requerimientos objeto de desarrollo definido en el Análisis de Requerimientos de Sistema, que le será facilitado al adjudicatario por la DGTSI.

Una vez realizados los trabajos, la aplicación será testada por el grupo de trabajo que a tal fin se defina así como por la OTGS quien además realizará una auditoría, realizando las pruebas de usuario y de sistemas que se estimen oportunas para verificar la fiabilidad de los resultados y del rendimiento obtenido. Los errores detectados en estas pruebas serán corregidos por el adjudicatario como parte del trabajo, sin coste adicional.

6. PLANIFICACIÓN Y ORGANIZACIÓN

Sin perjuicio de la documentación administrativa y la acreditativa de la experiencia de la empresa licitadora en labores similares a las aquí solicitadas, la empresa adjudicataria 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, donde figure:

- Diagrama temporal de actividades (cronograma de tareas)
- Organigrama del equipo de trabajo, especificando las funciones y responsabilidades de cada uno de sus integrantes, por categoría profesional, de acuerdo a los requerimientos del servicio

6.1 Mecanismos de seguimiento y control

El equipo de trabajo estará dirigido por un Responsable del Proyecto con dedicación estable, quien coordinará la realización de todas las tareas implicadas en el proyecto y actuará como interlocutor principal con los usuarios y la DGTSI.

La DGTSI establecerá un responsable para los aspectos organizativos, funcionales y técnicos. Esta persona actuará como interlocutor con la empresa contratada, y deberá acudir a cuantas reuniones de seguimiento se propongan.

La supervisión de funcionalidades del proyecto será llevada a cabo por el equipo de SIP de la DGTSI.

La supervisión de la calidad del proyecto en cuanto a código y normativa aplicada será llevada a cabo por la Oficina Técnica de la DGTSI.

La DGTSI establecerá todos aquellos procedimientos de control que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en los plazos como en la calidad final. Entre estos mecanismos se encuentran:

- Reuniones de seguimiento: a partir del plan de entregas requerido se realizarán reuniones, bien periódicas o coincidiendo con los puntos de

decisión, destinadas a revisar el grado de cumplimiento de las tareas planificadas, la entrega de productos, las resignaciones de personal, la validación de las programaciones de actividades a realizar, etc.

- Informes de situación y progreso que servirán para comunicar al equipo director de proyecto de la Administración, el estado actual de los trabajos, los objetivos alcanzados, las incidencias ocurridas, etc.
- Seguimiento de la documentación de gestión de proyectos y desarrollo.

7. PLAN DE ENTREGAS E HITOS DE CONTROL

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible, permitiéndonos realizar las tareas más importantes y urgente en primera instancia y dejar para un momento posterior aquellas con bajo nivel de prioridad.

La ejecución de este proyecto se establecerá en incrementos de forma que la entrega se pueda ir realizando por fases de entregas parciales.

El Plan de Entregas e Hitos de Control seguirá las tareas planificadas en el cronograma propuesto y marcado por la metodología vigente.

8. CONFIDENCIALIDAD, SEGURIDAD Y PROP. INTELECTUAL

En este pliego se describen funcionalidades, procedimientos, casos de uso, tipos de datos, etc. de los distintos Sistemas Informáticos del Departamento de Seguridad por ello se requiere, de todos aquellos que tengan acceso al presente documento, absoluta confidencialidad y reserva sobre la información contenida en el mismo.

Además, aquellas empresas que no resulten adjudicatarias no podrán conservarlo y deberán proceder a su destrucción.

8.1 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.

8.2 Normas de seguridad relativas a los S.I

El contratista 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.
- 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, 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.
- Devolver, al finalizar los trabajos o su asignación a los mismos, y en todo caso al término de la relación contractual/laboral, toda la documentación referente al proyecto (informes, propuestas, análisis, etc.).
- Acceso exclusivo a la información necesaria para el desempeño de las funciones encomendadas.
- Utilizar exclusivamente la password-clave a él asignada 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, el adjudicatario adquirirá los siguientes compromisos, que a continuación se describen en cuanto a materia de seguridad se refiere:

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

8.3 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.

Queda expresamente prohibida la utilización, para fines particulares, de cualquier material o información referente a los trabajos desarrollados, ya existentes y de proyectos internos o externos.

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.

9. 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 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
  - Manual de explotación que recogerá el conjunto de tareas que se deberán realizar para la correcta explotación del sistema.

10. GESTIÓN Y ADMINISTRACIÓN DEL SERVICIO

Con el objeto de verificar la garantía y calidad del proyecto se establecerá un Comité de seguimiento formado por el jefe de proyecto de la empresa adjudicataria y un equipo supervisor de la DGTSI encargado de controlar de forma continuada el cumplimiento de los objetivos especificados, tanto en los plazos como en la calidad final.

El adjudicatario será el responsable de realizar la gestión y seguimiento de las tareas de desarrollo encomendadas en el presente pliego de base técnicas de acuerdo a lo establecido en la normativa de Calidad definida para tal fin.

Desde el inicio del servicio, el adjudicatario deberá funcionar de manera autónoma, resolviendo adecuadamente y en los plazos marcados las peticiones de trabajo planificadas, gestionando los recursos y obteniendo los indicadores e informes establecidos para las reuniones de seguimiento.

El adjudicatario será el responsable de adecuar el personal técnico necesario en función de las necesidades poniendo a disposición del contratante aquéllos mejor cualificados para el tipo de servicio que se esté demandando. La designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de la Administración, y en este caso, el adjudicatario se obliga a proponer otras personas. La elección por la Administración de ésas u otras personas no alterará en ningún caso el precio ofertado por la adjudicataria.

Deberá facilitar al Comité de seguimiento con la frecuencia que se establezca, los informes e indicadores definidos por el Departamento de Seguridad.

Entre los indicadores se deberán recoger aquellos que sirven de referencia para medir el nivel de cumplimiento de los acuerdos de nivel de servicio.

Al objeto de facilitar todo ello, se establece la obligación de cumplimentar adecuadamente la información requerida sobre las herramientas de gestión del Departamento de Seguridad, como soporte para la gestión de la tarea a desempeñar (incidencias, partes de trabajo, etc.).

11. LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de trabajo, por defecto, serán las instalaciones de la DGTSI en su sede de Larrauri Mendotxe bidea, 18 en Erandio (Bizkaia).