



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

¡BERRITU: REDISEÑO APLICACIONES WEB

PLIEGO DE PRESCRIPCIONES TÉCNICAS



TABLA DE CONTENIDOS

	Página
1. INTRODUCCIÓN	2
2. ALCANCE DEL CONTRATO.....	3
3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS.....	5
4. EJECUCIÓN DEL CONTRATO	24
4.1. PLANIFICACIÓN Y ORGANIZACIÓN.....	24
4.2. ENTORNO TECNOLÓGICO.....	24
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO	26
4.4. GESTIÓN DE LA CALIDAD	27
4.5. COBERTURA EN PRUEBAS AUTOMATIZADAS.....	30
4.6. CONSIDERACIONES TÉCNICAS Y DE RENDIMIENTO	30
4.7. GENERACIÓN DE DOCUMENTOS PDF.....	31
4.8. DOCUMENTACIÓN Y FORMACIÓN A USUARIOS/AS	31
4.9. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN.....	31
4.10. DOCUMENTACIÓN NO SEXISTA.....	32
4.11. REGISTROS, NOTIFICACIONES E INVENTARIOS.....	32
4.12. LUGAR DE EJECUCIÓN DEL CONTRATO.	32
5. DOCUMENTOS ANEXOS.....	33
ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN.....	33

1. INTRODUCCIÓN

El Decreto 318/2024, de 29 de octubre, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad del Gobierno Vasco, en su artículo 18, establece que corresponde a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos (DGTSI) lo referente a la planificación, elaboración, desarrollo, ejecución, gestión y mantenimiento de los sistemas de información y telecomunicaciones destinados a actividades de seguridad pública. Es en virtud de dicha competencia que se acomete el presente expediente.

Con el fin de mejorar los servicios prestados y de potenciar el uso de estándares oficiales y de mercado generando una situación en la que no exista una dependencia exclusiva de un único proveedor, desde la DGTSI se ha dado comienzo a una serie de iniciativas, encuadradas en el proyecto denominado iBerritu, con el objeto de realizar la migración de la plataforma IBM a sistemas abiertos. En este sentido, en el año 2020 se finalizó la migración de los portales públicos del DSGV al producto Liferay DXP y servidores WebLogic para la parte de negocio. En el año 2021 se comenzó la migración de la extranet a la misma plataforma, anteriormente indicada. En el año 2023 se comenzó la migración de contenidos y de una serie de aplicaciones piloto incluidas en la intranet departamental a la referida plataforma Liferay DXP y servidores Weblogic, cuya finalización está prevista en este 2025. Dentro de esta iniciativa, se incluye este expediente cuyo objetivo es la contratación de los servicios para el rediseño, migración, reingeniería y evolución tecnológica de tres aplicaciones de la intranet corporativa ajustándose a los estándares del nuevo paradigma de desarrollo.

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 pliego tiene por objeto la contratación de las tareas que permitan realizar el rediseño, revisión y adaptación de las aplicaciones que se indican más adelante del entorno tecnológico actual, basado en IBM WebSphere, garantizando su correcto funcionamiento tras la actualización del entorno tecnológico sobre el que van a estar soportadas. Deberá incluir la reingeniería de las capas de presentación, integración y negocio, garantizándose en todo momento, que en este proceso de reingeniería y migración no se produce pérdida de funcionalidad ni de rendimiento.

El nuevo código implantado deberá ajustarse a los nuevos requisitos de arquitectura, estilos, seguridad y calidad establecidos por la DGTSI.

A continuación, se identifican las aplicaciones a rediseñar objeto de esta contratación:

- **A13: SMS:** Esta aplicación tiene como objetivos principales el envío de mensajes bien a de SMS's o de correos electrónicos (Email). Estos envíos pueden ser inmediatos, diferidos, combinados. Para poder realizar esta difusión, son necesarios procesos para la gestión y mantenimiento de las siguientes entidades: abonados, grupos de abonados, usuarios de la aplicación y entidades. Adicionalmente, la aplicación cuenta con una consulta histórica del envío de SMS/Email históricos. Por cada envío se recoge, además, el acuse de recibo o su expiración.
- **A21: Expedientes de Contratación:** Esta aplicación permite tramitar los diferentes tipos de expedientes de contratación (contratación menor, negociado sin publicidad, concurso restringido, concurso abierto, convalidación, incidencia, y emergencia). La tramitación de expedientes engloba el ciclo de vida del expediente, desde su inicio en una Área Gestora hasta su cierre en Contratación. La aplicación permite el manejo de los documentos asociados a cada expediente. Además, de la gestión permite la consulta y seguimiento de los expedientes.

- **A22: Gestión Resoluciones de RRHH:** Esta aplicación permite realizar la gestión de las reclamaciones y recursos, así como proporcionar una gestión centralizada de las notificaciones. También dispone de un registro de sentencias de asuntos de interés, así como gestionar las consultas internas y las solicitudes de ciertos procedimientos. A la funcionalidad actual, se debe incorporar las siguientes nuevas:
 - Facilitar la presentación de escritos por los diferentes colectivos afectados a través de la extranet “Segurgune”. Para ello, será necesaria la publicación en dicho portal de un módulo que dé respuesta a esta necesidad.
 - Sustituir el proceso actual de notificación de las resoluciones manual a través de un medio telemático.

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS

3.1.1 Aspectos generales a todas las aplicaciones

El proceso de rediseño, además, de mejoras en la gestión de la funcionalidad deberá contemplar la migración de plataforma tecnológica y la reingeniería de los procesos, por tanto, se deberá cumplir con los siguientes requisitos:

- Rediseño de las funcionalidades y lógica de negocio, de forma que la aplicación sea más sencilla, intuitiva y usable facilitando a la persona usuaria la interacción con el sistema de forma fácil.
- adaptación y actualización de los desarrollos a la versión 8 o superior del lenguaje de desarrollo Java.
- adaptación y actualización de los desarrollos portlet a la especificación Portlet 3.0 (JRS 362) con el estándar Java Server Faces 2.2
- adaptación y actualización de los desarrollos Primefaces 6.1 a Primefaces 11.0 u otra tecnología según se establezca en normativa de desarrollo.
- adaptación y actualización de los desarrollos Java EE 1.3, 1.4, 5 y 6 a la especificación Java EE8
- eliminación de la denominada “deuda técnica”
- refactorización del código, con el objetivo de hacerlo más legible, mantenible, eficiente y menos complejo
- sustituir el uso de librerías internas como “BIDEA” y “OINARRI” por su equivalente más actual “GIDA” (a modo de ejemplo, actualmente se está utilizando el componente de control de flujo de B72-Bidea; será, por tanto, necesario modificarlo para utilizar el componente de control de flujo de L42)
- evolución de la integración con otros servicios o aplicaciones mediante servicios web SOAP y/o REST con propagación de identidad mediante estándares abiertos como OAuth2, JWT o SAML 2.0

- adaptación de scripts de ejecución de procesos batch invocados por el aplicativo Control-M
- migración de informes generados con Apache FOP o JasperReports a la versión más reciente de JasperReports. En los casos, en los que así lo determine la DGTSI la migración se hará mediante el uso de IberDok. Esta decisión se tomará de forma conjunta con la DGTSI en función de las necesidades funcionales de cada aplicación.

3.1.2 Migración de la capa de presentación

Los aplicativos webs de la actual intranet del Departamento están desarrollados con las siguientes tecnologías: Portlet 1.1 con Struts Portlet Framework 1.1 y Servlets AJAX.

Dichos aplicativos se integran con las actuales capas de negocio e integración a través de peticiones SOAP y RMI (A13), y Apache Struts REST y JSON (en 21 y A22).

El acceso a las aplicaciones web está protegido por grupos del servicio de directorio corporativo.

Además, las aplicaciones protegen sus recursos (pestañas, botones, acciones de negocio, etc.) con un segundo nivel que asigna privilegios a dichos recursos por medio de listas de control de accesos (ACL) de cara al soporte de distintos perfiles de usuario/a.

Las aplicaciones deberán mantener el bilingüismo (euskera y castellano) y ser compatibles y usables con los siguientes navegadores web (en orden de prioridad): Microsoft Edge y Chrome 100 o superior, así como cumplir con las normativas de accesibilidad a sitios web.

En los casos, que la aplicación no tenga toda la funcionalidad bilingüe se deberá identificar y proponer textos traducidos al euskera para su validación e incorporación a las nuevas aplicaciones.

3.1.3 Migración de la capa de negocio

En el entorno actual, se dispone de dos clústeres de servidores de negocio WAS:

- Clúster de corta: procesos de negocio con un tiempo máximo de transacción de 120 segundos que se consumen desde aplicaciones web, el ESB Oracle Service Bus; y el IBM ACE (App Connect Enterprise).

- Clúster de larga: procesos de negocio que por sus características requieren de un tiempo de transacción elevado, por ejemplo, procesos batch. Estos procesos se activan de forma planificada desde la aplicación CONTROL-M o bien por la recepción de mensajería JMS.

En el entorno destino Weblogic se dispondrá de una arquitectura equivalente de clústeres de negocio.

Los servidores de aplicaciones mantienen aplicativos de las siguientes tecnologías:

- EARs de aplicaciones y servicios horizontales
- WAR aplicaciones web
- EJBs 2.x, 3.x
- Servicios web SOAP Axis 1.x
- RAR conectores JCA
- Procesos batch

3.1.4 Migración de la capa de integración

Los actuales aplicativos de la capa de integración, que se utilizan, por ejemplo, para integrar desarrollos Java EE con aplicativos del mainframe Host, se ejecutan sobre la plataforma IBM App Connect Enterprise. Es objeto de esta iniciativa la reingeniería de dichos aplicativos que se migrarán a los entornos Oracle Service Bus, Control-M y/o aplicativos Java EE dependiendo de la funcionalidad demandada.

Entre las distintas funcionalidades que cubren los actuales aplicativos están las siguientes:

- publicación de servicios vía servicio web o cola JMS/MQ
- integración con Host vía colas IBM MQ
- transformación de datos entre los distintos servicios y aplicaciones
- soporte de flujos asíncronos
- envío de ficheros vía FTP/SFTP
- publicación y suscripción de mensajes

- proceso de ficheros, incluyendo la activación de un flujo a partir de la existencia de un fichero
- envío de alertas SNMP

3.1.5 Migración de datos

Las aplicaciones del Departamento persisten sus datos en Oracle RAC.

En caso de ser necesario un rediseño de BBDD, se deberá valorar y aprobar por la DGTSI. En caso de llevarse a cabo, el adjudicatario deberá contemplar la migración de los datos actuales a la nueva estructura que se defina. Además, cualquier modificación sobre la estructura de las tablas deberá ser comunicada al responsable de la DGTSI que se designe de cara a evaluar su impacto sobre los procesos de DataWarehouse existentes.

3.1.6 Aplicaciones a rediseñar / migrar

Las aplicaciones a rediseñar son las que se indican a continuación, que se pasan a describir.

3.1.6.1. A13 – SMS

La presente aplicación tiene como objetivos principales el envío de mensajes bien de SMS's o de correos electrónicos (Email). Estos envíos pueden ser inmediatos, diferidos, combinados. Para poder realizar esta difusión, son necesarios procesos para la gestión y mantenimiento de las siguientes entidades: abonados, grupos de abonados, usuarios de la aplicación y entidades. Adicionalmente, la aplicación cuenta con una consulta histórica del envío de SMS/Email históricos. Por cada envío se recoge, además, el acuse de recibo o su expiración.

La aplicación cuenta con varias pantallas:

- Inicio: pantalla de presentación y descripción de la aplicación.
- Gestión de envíos:

- Consulta de envíos: permite realizar búsquedas de envíos de SMS o EMAIL en el registro histórico mediante distintos filtros.
- Enviar Email: permite el envío de EMAIL mediante un formulario.
- Enviar SMS: permite el envío de SMS mediante un formulario diferente para cada tipo de envío (inmediato, diferido, reenvío o combinado).
- Entidades: permite realizar búsquedas de entidades por nombre, y permite el mantenimiento de las entidades existentes, así como la creación de nuevas entidades.
- Usuarios: permite realizar búsquedas de usuarios mediante distintos filtros.
- Gestión de abonados:
 - Abonados: permite realizar búsquedas de abonados mediante distintos filtros, y permite el alta de nuevos abonados.
 - Grupos: permite realizar búsquedas de grupos mediante distintos filtros, y permite el alta de nuevos grupos.
 - Carga Excel: permite la carga de abonados mediante la subida de un fichero Excel.
- Gestión de históricos: permite realizar búsquedas de SMS en el histórico mediante distintos filtros.
- Consulta de abonados: permite realizar búsquedas de abonados mediante distintos filtros.

En el rediseño se tendrán en cuenta mejoras en la navegación de pantallas y se ajustarán los tamaños de los campos para facilitar la visualización de todos los campos. Así mismo, se debe mejorar la usabilidad en la visualización y tratamiento de documentos. Así mismo, puede haber variaciones en cuanto a algunos de los campos a presentar o incorporar en las diferentes funcionalidades de la aplicación.

Dentro de este proyecto si incluye la exposición de un servicio web para permitir la integración del resto de aplicaciones del Departamento con la plataforma de mensajería. La implementación de esta integración debe hacerse a través de la plataforma MENTES.

- smsEnvio: permite realizar el envío de SMS a través de Mentos mediante servicio web. Método expuesto enviarSMS.
- smsRecepcion: permite la recepción de acuses de recibo de SMS y MMS de Mentos. Métodos expuestos deliveryReport, deliveryReportExtended, mmsDelivery, smsDelivery.
- smsWebService: permite realizar el envío de SMS mediante servicio web. Métodos expuestos insertSMSWS, buscarEnvioWS.

La implementación de este envío a la plataforma MENTES se hará a través de colas JMS. Si durante las pruebas de rendimiento, se detectase que es posible realizar los envíos directamente a MENTES sin necesidad de usar colas JMS, se procederá a ajustar este proceso.

Además, de las funcionalidades actuales, se expondrán los siguientes nuevos servicios, internos para consumo de aplicaciones y que son ajenos a la plataforma MENTES:

- getEntidades: permite obtener las entidades disponibles para un usuario.
- getEmisores: permite obtener los emisores disponibles para una entidad y un usuario.
- getGrupos: permite obtener los grupos disponibles para una entidad.
- getDestinatarios: permite obtener los miembros de un grupo.

La administración de esta aplicación puede ser realizada por los usuarios administradores, a través de la aplicación “administración delegada” definida para tal fin. Será necesario revisar, si como consecuencia de la migración o rediseño, es necesario hacer algún ajuste en la configuración de la administración delegada.

Tecnologías e Integración

Tecnologías negocio	Java 1.8, J2EE 1.7, EJB 3.2
Tecnologías de presentación	Java 1.8, Portlet 3.0, Primefaces 11.0 u otra tecnología según se establezca en normativa de desarrollo

Persistencia	Oracle 19c – JPA 2.1
Integraciones	Integración con el Servicio Horizontal de auditoría publicado por la librería GIDA. Integración con el servicio de Mentes utilizando colas JMS
Seguridad	Acceso restringido. Existen 3 roles de seguridad (administrador, operador y supervisor).
LOPD	Todas las acciones de alta/modificación/baja/consulta sobre los SMS/Email, entidades, emisores y abonados deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.1.6.2. A21 – Expedientes contratación

La aplicación de Gestión de Expedientes permite tramitar los diferentes tipos de expedientes de contratación. La tramitación de expedientes engloba el ciclo de vida del expediente, desde su inicio en una Área Gestora hasta su cierre en Contratación. La aplicación permitirá el manejo de una forma fácil y eficaz de los documentos asociados a cada tipo de expediente. También facilita la consulta y seguimiento de los expedientes.

Los tipos de tramitación que el sistema gestiona son los siguientes:

- Contratación Menor
- Negociado sin Publicidad
- Concurso Restringido
- Concurso Abierto
- Convalidación
- Incidencia
- Emergencia

En el proceso de tramitación del expediente están involucradas tres áreas claramente definidas. Cada una de ellas es responsable de realizar diferentes acciones dentro del ciclo de vida del expediente.

- Áreas Gestoras
- Área Contratación
- Área Contabilidad

Durante el proceso de tramitación el expediente puede pasar por los siguientes estados:

- Inicio de Expediente
- Autorización Responsable Contratación
- Inicio expediente en Contratación
- Inicio Expediente en Contabilidad
- Elaboración Orden Adjudicación
- Liberación del Expediente
- Finalización de la tramitación del Expediente

Según el estado en el que se encuentre el expediente y el perfil de acceso del usuario, la aplicación muestra un menú formado por diversas opciones: Nuevo Expediente, Bandeja Trabajo, Bandeja de Áreas Gestoras, Mis Expedientes, Consultas, Transferir. Cada una de estas acciones permite localizar y tramitar los expedientes.

Además, la aplicación presenta las siguientes pantallas:

- Inicio: descripción de la aplicación.
- Nuevo expediente: disponible para los perfiles Área Gestora, Usuario Contratación y Usuario Contabilidad. Permite la creación de un nuevo expediente.
- Bandeja de trabajo TR: disponible para los perfiles Área Gestora, Responsable Contratación, Usuario Contratación y Usuario Contabilidad. Permite visualizar un listado con los expedientes, para los que el usuario puede realizar algún trámite.

- Bandeja de trabajo AG: disponible para los perfiles Usuario Contratación y Usuario Contabilidad. Permite visualizar un listado con los expedientes para los que el usuario puede realizar algún trámite, como si fuera un Área Gestora.
- Mis expedientes: disponible para los perfiles Área Gestora, Responsable Contratación, Usuario Contratación y Usuario Contabilidad. Permite visualizar un listado con todos los Expedientes, sobre los que tenga permisos, abiertos de las áreas gestoras a las que pertenece el usuario.
- Consultas: disponible para los perfiles Área Gestora, Responsable Contratación, Usuario Contratación y Usuario Contabilidad. Permite realizar una búsqueda sobre todos los expedientes (abiertos o cerrados) a los que se tienen permisos de visualización. Además, también permite buscar documentos asociados al expediente, y ver su contenido.
- Informes: permite generar los informes en formato PDF sobre todos los expedientes (abiertos o cerrados) a los que se tienen permisos de visualización.
- Transferir: disponible para el perfil Responsable Contratación. Permite transferir expedientes asignados a un usuario de Contratación, a otro usuario.
- Mantenimiento: disponible para el perfil Administrador. Permite realizar los mantenimientos de las tablas maestras de la aplicación (CACs, CRCs, Plantillas, Destino final y Sistemas).

En la visualización y consulta se deberá tener en cuenta las limitaciones de aquellos expedientes categorizados como secretos, que solo estarán accesibles a determinados perfiles o incluso gestores.

Forma parte de la contratación la revisión de la funcionalidad con el fin de determinar acciones de mejora, no solo en la usabilidad de la aplicación sino también en la propia funcionalidad y flujos de trabajo de la aplicación.



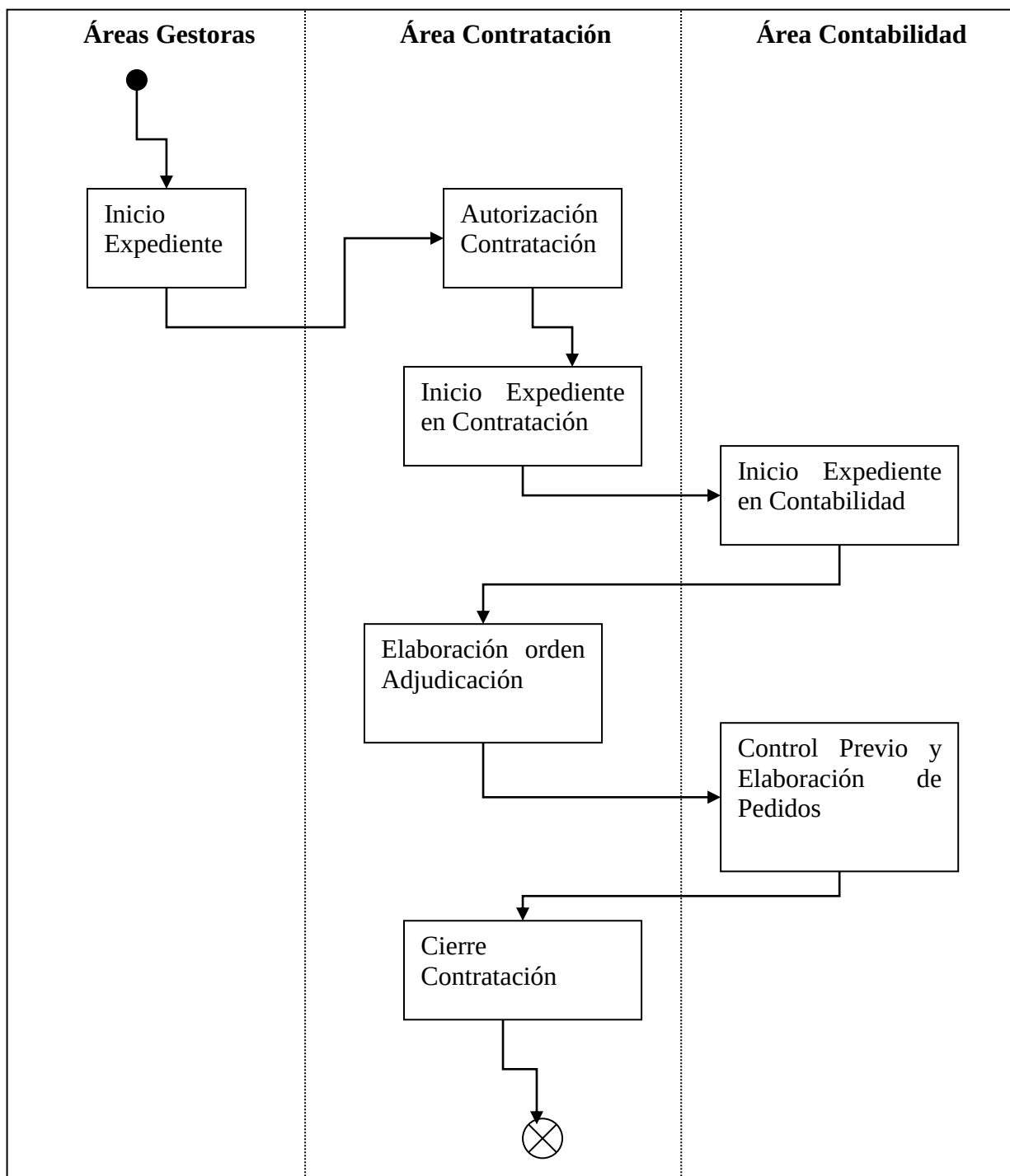
Como nuevo requisito se deberá contemplar la posibilidad de que determinados expedientes que, bien en función del tipo de tramitación o de otro criterio, se quiera automatizar su integración con la plataforma del Gobierno Vasco de contratación para los poderes adjudicadores, con el fin de facilitar el trámite de publicación en el Perfil del Contratante. Para ello, se deberá hacer uso de los WS que, para tal fin, expone el Gobierno Vasco a través de EuskalSarea.

Esta aplicación dispone de Cuadros de Mando, por lo que cualquier modificación en la definición de las tablas se debe tener en cuenta para valorar el impacto en los cuadros de mando actualmente definidos.

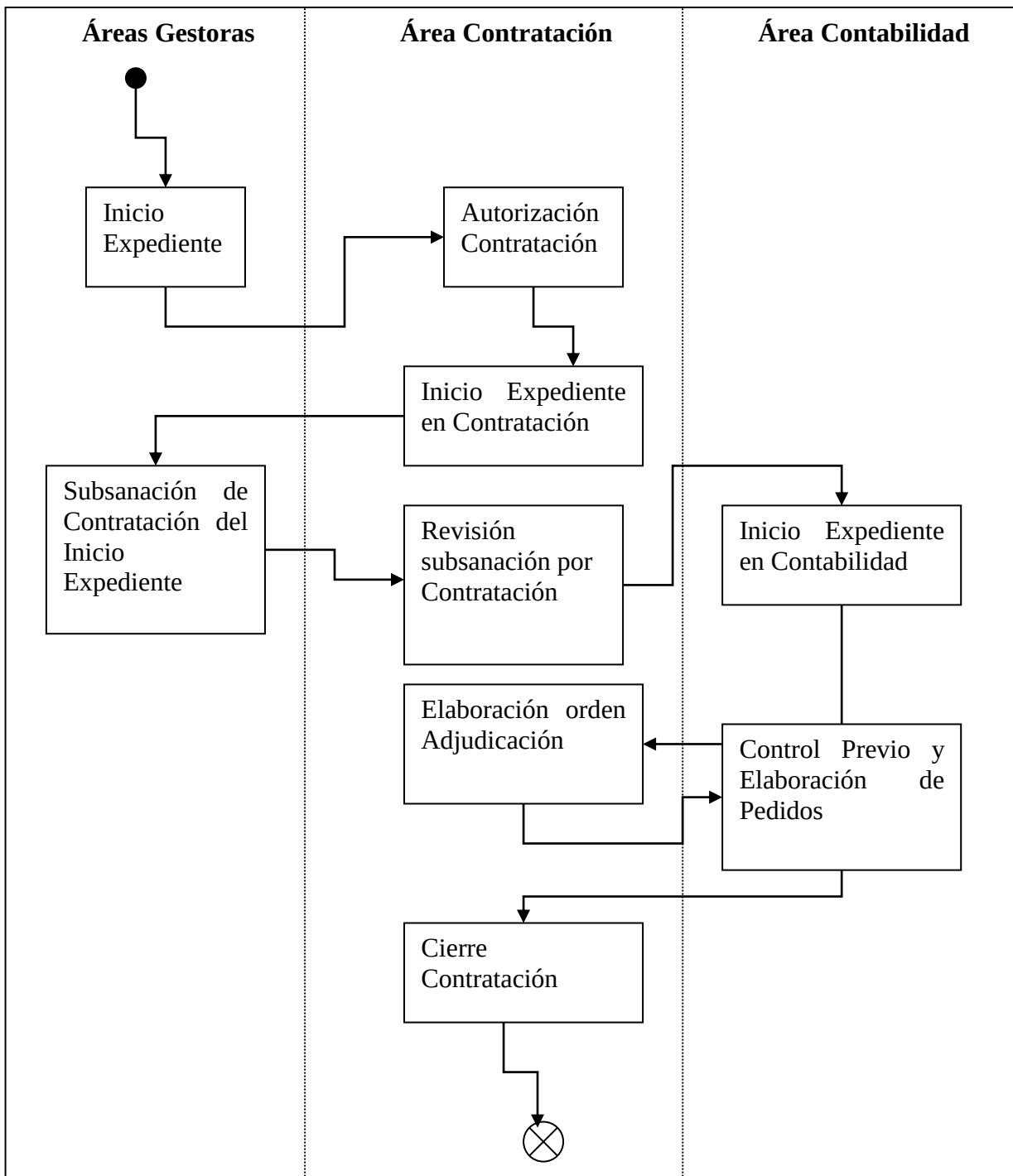
Diagramas de secuencia del Proceso de Tramitación

A modo de ejemplo, se incluyen 3 diagramas de secuencia.

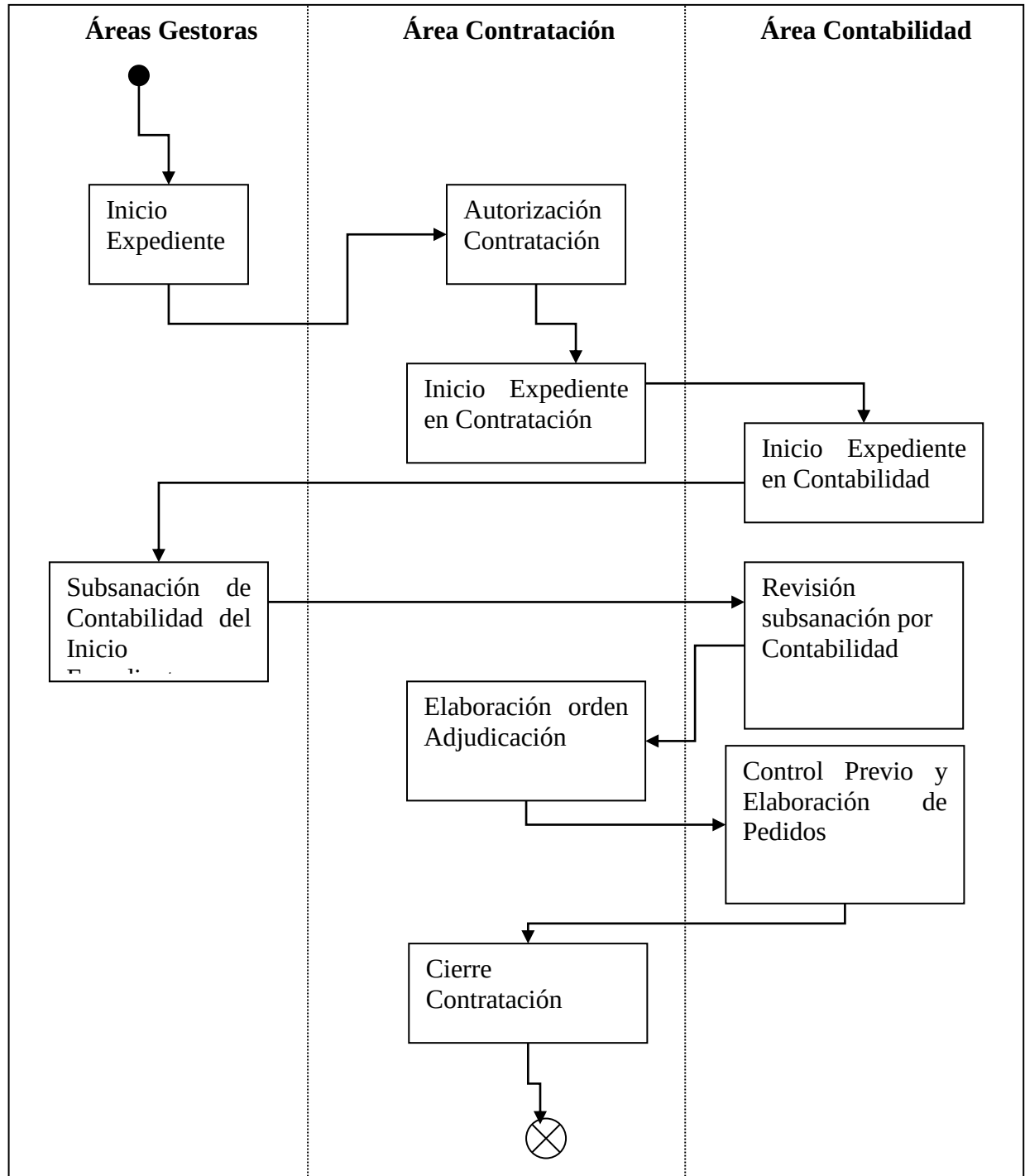
- **Diagrama de Secuencia Flujo normal**, muestra la secuencia general de estados para el proceso de tramitación de un expediente.



- **Diagrama de Secuencia Flujo con Solicitud Subsanación de Contratación,** muestra los estados por los que pasa un expediente cuando se requiere una subsanación detectada en Contratación.



- **Diagrama de Secuencia Flujo con Solicitud Subsanación de Contabilidad**, muestra los estados por los que pasa un expediente cuando se requiere una subsanación detectada en Contabilidad.



Tecnologías e Integración

Tecnologías negocio	Java 1.8, J2EE 1.7, EJB 3.2
Tecnologías de presentación	Java 1.8, Portlet 3.0, Primefaces 11.0 u otra tecnología según se establezca en normativa de desarrollo
Persistencia	Oracle 19c – JPA 2.1
Integraciones	Integración con el Servicio Horizontal de auditoría publicado por la librería GIDA. Integración con el Servicio Horizontal “Kudok” de Gestión Documental (se deberán eliminar la subidas asíncronas de documentación). Integración con SAP (Aurrera!) a través de los WS existentes. Perfil del Contratante: Nueva integración
Seguridad	Acceso restringido. Existen 5 perfiles de seguridad: • Perfil Áreas Gestoras • Perfil Responsable Contratación • Perfil Área Contratación • Perfil Área Contabilidad • Perfil Administrador

3.1.6.3. A22 – Gestor Resolución RRHH

Esta aplicación actualmente, permite realizar la gestión de las reclamaciones y recursos, así como proporcionar una gestión centralizada de las notificaciones. También dispone de un registro de sentencias de asuntos de interés, así mismo, permite gestionar las consultas internas y las solicitudes de ciertos procedimientos. La funcionalidad de “Asuntos” ha quedado en desuso y ya no será necesaria su migración.

A la funcionalidad actual, se deben incorporar estos dos nuevos requisitos:

- Facilitar la presentación de escritos por los diferentes colectivos afectados a través de la extranet “Segurgune”. Para ello, será necesaria la publicación en dicho portal de un módulo que dé respuesta a esta necesidad.
- Sustituir el proceso actual de notificación de las resoluciones manual a través de un medio telemático.

Los asuntos a abordar por esta aplicación son reclamaciones, recursos, sentencias y resoluciones de procedimientos, así como cualquier otra tramitación que se requiera de la Dirección de Recursos Humanos.

Será, por tanto, necesario revisar los flujos de tramitación y adecuarlos a las nuevas necesidades de los nuevos tipos de asuntos que pueden surgir, siendo posible la aparición de nuevos actores en la tramitación.

Las pantallas de la aplicación son las siguientes:

- Inicio: presenta descripción de la aplicación.
- Administración: permite configurar las diferentes tablas maestras y configuraciones existentes en la aplicación.
- Cartera: permite acceder a los recursos y sentencias en curso a los que se tenga acceso para proseguir con su flujo, ordenados por estado o por fecha.
- Consultas: permite acceder a las sentencias y recursos ya creados mediante un buscador.

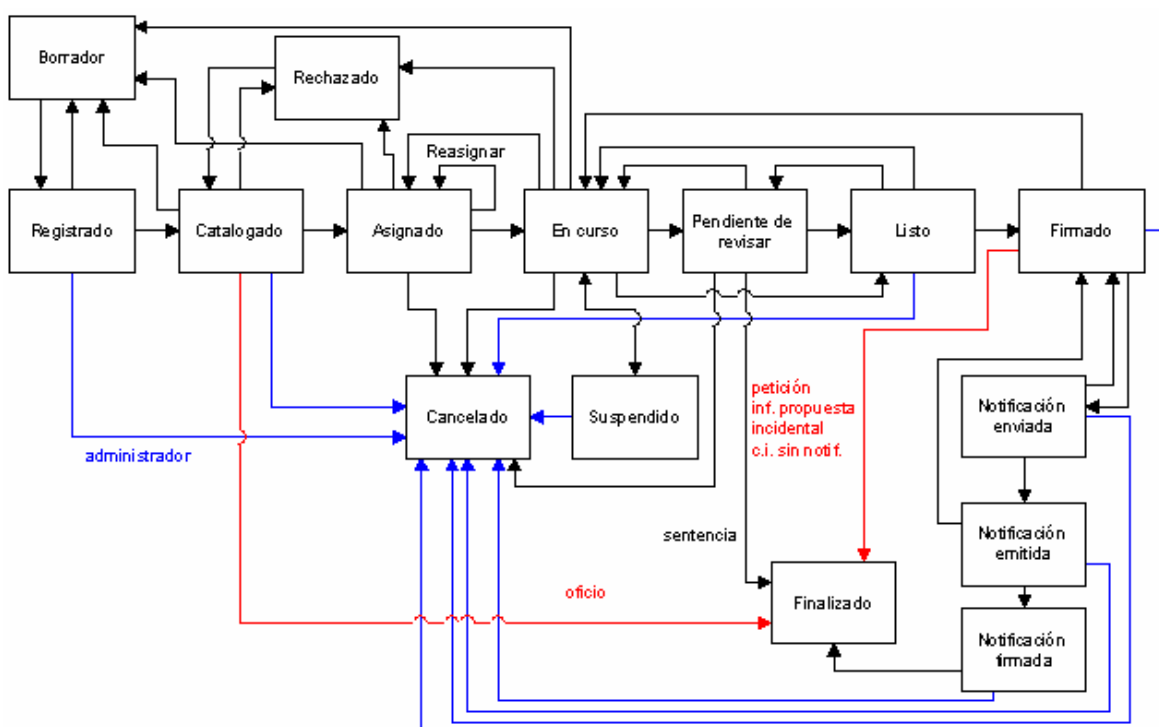
El flujo habitual del trámite de un expediente, que deberá ser revisado, es el siguiente:

Borrador → Registrado → Catalogado → Asignado → En Curso → Pendiente de -revisar → Listo → Firmado → Notificación enviada → Notificación emitida → Notificación firmada → Finalizado.

Habrà que revisar en este flujo el impacto de la integración con la persona peticionaria desde la extranet, así como la migración de la notificación a formato electrónico.

Además, existen transiciones extraordinarias que pueden ser ejecutadas en ciertas condiciones, como, por ejemplo, un usuario con rol administrador puede pasar un expediente a estado Cancelado según determinadas condiciones. También pueden darse situaciones concretas que conlleven una transición especial por los estados, no respondiendo al flujo estándar o habitual.

La siguiente imagen ilustra de una forma más clara las transiciones existentes (incluyendo las menos habituales y extraordinarias) en este sistema de tramitación de documentos.



En el rediseño de la aplicación puede haber variaciones en los flujos establecidos.

Cada usuario puede tener asignado uno o más de los siguientes roles asociados con las transiciones anteriormente descritas:

- Registrador
- Notificador
- Catalogador
- Responsable
- Tramitador
- Consulta

- Firmante
- Administrador

Otro aspecto a tener en cuenta en el rediseño de la aplicación:

- Será necesario revisar la definición de las bases de datos, con el fin de normalizar datos, así como su tipología. A modo de ejemplo, es necesario cambiar los campos de fecha a tipo DATE, ya que se han encontrado algunos campos cuyo tipo de datos son VARCHAR.

Tecnologías e Integración

Tecnologías negocio	Java 1.8, J2EE 1.7, EJB 3.2
Tecnologías de presentación	Java 1.8, Portlet 3.0, Primefaces 11.0 u u otra tecnología según se establezca en normativa de desarrollo
Persistencia	Oracle 19c – JPA 2.1
Integraciones	Integración con el Servicio Horizontal “Kudok” de Gestión Documental. Integración con Iberdok para la generación de documentos. Será necesaria la migración de plantillas ya existentes a Iberdok, así como la creación de nuevas, en caso necesario. Se valorará la integración con Sede Electrónica, para el envío de la notificación y recepción del acuse de recibo. Integración con el Servicio Horizontal de auditoría publicado por la librería GIDA.

Seguridad	Acceso restringido. Diferentes perfiles de seguridad combinables en un mismo usuario: • Registrador • Notificador • Catalogador • Responsable • Tramitador • Consulta • Firmante • Administrador
LOPD	Todas las acciones realizadas deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.1.7 Características básicas

Las aplicaciones a rediseñar objeto de este pliego deberán contemplar las siguientes características básicas:

- **Seguridad:**

Las funcionalidades expuestas y limitadas por la seguridad restringirán el acceso en función de la persona conectada al sistema.

- **Multilingüismo:**

Las aplicaciones de portal han de contemplar la posibilidad de selección del idioma de navegación (Euskera o Castellano)

- **Accesibilidad:**

Las aplicaciones de portal cumplirán con los estándares tecnológicos y los requerimientos de accesibilidad establecidos por la DGTSI.

- **Servicios:**

Las aplicaciones de portal se integrarán con los servicios horizontales definidos según necesidades del análisis (gestor documental, auditoría, correo, ...).

- **Normativa:**

El desarrollo de las aplicaciones deberá seguir las normativas establecidas por la DGTSI.



- **Usabilidad:**

Las aplicaciones de portal deberán seguir la guía de estilos que se proporcione por la DGTSI y ser responsive.

- **Navegadores:**

Se deberá garantizar que sea accesible desde los navegadores basados en Chromium versiones 100 o superiores, en concreto con los navegadores Google Chrome y Microsoft Edge.

4. EJECUCIÓN DEL CONTRATO

4.1. Planificación y organización

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

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible, permitiendo el correcto ajuste temporal de todas las tareas que constituyen el contrato y permitiendo la priorización de las tareas más importante y/o 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 proporcionará a la empresa adjudicataria toda la información necesaria para el desarrollo de este pliego en el nuevo entorno tecnológico.

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

El entorno tecnológico es el que se cita a continuación, si bien, a lo largo de la vida del contrato pueden cambiar tanto las versiones como los productos que se indican.

Gestión de portales y Servidor de aplicaciones:

- Desarrollo de Portlets en el portal Liferay DXP 7.3 o superior sobre JBoss 7.3
- 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 o superior)
 - Liferay MVC Portlet
 - EJB 3.2 + JPA 2.1
 - OSGi R6 bundles

Gestión documental

- IBM DB2 Content Manager v8.5

Mensajería y bus de integración

- Mensajería JMS/MQ y bus de integración
- Oracle Service Bus 12.2.1.4
- Mensajería IBM Websphere MQ 9.2

Servidor de Bases de datos:

- Oracle 12.2 RAC

Automatización de procesos

- Control-M

Repositorios

- Azure DevOps Server 2020
- Microsoft SharePoint 2016 o superior

Suite de seguridad:

- Microsoft TMG 2010

- Oracle HTTP Server 12.2.1.4
- Oracle Access Manager 12.2.1.4

Frameworks y estándares:

- Todos los desarrollos deben ser compatibles con la versión 8 o superior de la JDK
- Librerías internas “GIDA” para funcionalidades comunes: trazas de aplicación, consulta de propiedades, credenciales de usuario, etc.
- La DGTSI dispone de un conjunto de servicios horizontales y componentes reutilizables para dar solución a las necesidades comunes identificadas por las aplicaciones, que deberán usar las aplicaciones a rediseñar siempre que sea posible.

4.3. Cualificación técnica del equipo de trabajo

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

Jefe de Proyecto

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

Analista / Desarrollador

- Elaboración de las especificaciones técnicas de la solución.

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

Diseñador gráfico de aplicaciones

- Elaboración de los prototipos y diseños gráficos de las interfases
- Optimización de la navegación y la interacción de las personas usuarias con la aplicación, asegurando que sea intuitiva y eficiente.
- Desarrollo del front-end para implementar el diseño en la aplicación, asegurando que funcione correctamente en diferentes dispositivos y navegadores y garantizando una solución responsive

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 incluido en el ámbito del presente pliego de prescripciones 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 y de regresión que eviten la introducción de un nuevo defecto al intentar reparar el inicialmente o la reparación incorrecta del error que se pretendía corregir.
- Pruebas de integración. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.

- Pruebas de sistema. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.
- Pruebas de carga o rendimiento, en los casos, que se establezcan en función de la modificación realizada.

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

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

El número de no conformidades tanto menores como mayores que superen el nivel de cumplimiento exigido podrá llevar asociado la aplicación de penalizaciones, salvo justificación pormenorizada del proveedor en la revisión, y aceptación de la misma por parte del responsable de la 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.

El código entregado como resultado de la ejecución de este contrato deberá cumplir tanto los requisitos de arquitectura como las normativas de desarrollo que establezca la DGTSI, 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 realizará una revisión automática del código, así como una posible inspección manual del mismo.

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

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

a) Proyecto

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

b) Por aplicación

- Documento de requisitos con la identificación de los requisitos funcionales/no funcionales del Sistema.
- Análisis funcional con la descripción 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. Se entregarán de las funcionalidades más relevantes.
- Arquitectura del sistema con el diseño a de la arquitectura y descripción de los componentes de la arquitectura junto sus relaciones.
- Diseño físico de datos con el esquema físico de la base de datos, descripción de los objetos utilizados y volumetría estimada de las tablas e índices de BBDD
- Interface de usuario o prototipo de la aplicación, con los interfaces del usuario para cada módulo del 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 para la migración de datos y/o cargas iniciales, en caso de ser necesario.
- Manual de uso, según perfil. Documento que recoja en detalle cómo usar la aplicación según los diferentes perfiles existentes, así como posibles videos o píldoras formativas de las partes más comunes de la aplicación.

- 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. 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.

4.6. Consideraciones técnicas y de rendimiento

Las aplicaciones deberán tener un tiempo de respuesta adecuado a cada caso y deberá ser al menos similar o mejor al actual.

El manejo de datos deberá incluir políticas y procedimientos de cacheo adecuados a su naturaleza (datos efímeros, datos longevos, etc.)

Deberá evitarse en lo posible el uso de sesiones HTTP para almacenamiento de datos.

4.7. Generación de documentos PDF

Las aplicaciones que incluyen la capacidad de generar documentos en formato PDF para el/la usuario/a utilizan librerías como Apache FOP, iText o versiones antiguas de Jasper Reports.

Los procesos de creación de documentos deberán hacer uso de la librería Jasper Reports definida en la nueva plataforma, eliminando el uso de las librerías anteriores, y para los casos en los que se utiliza iText hacer uso de la librería LibrePDF.

Además, en el caso de aplicativos que requieran gestión de plantillas por parte de la persona usuaria final o tengan iteración con la persona, que en la plataforma anterior se cubría con el software Aspose, deberán hacer uso de IberDok para la gestión y creación de documentos.

4.8. Documentación y formación a usuarios/as

El proyecto debe incluir además de la documentación típica del ciclo de vida de un proyecto, manuales de uso y jornadas de formación para que las personas usuarias conozcan las nuevas aplicaciones, herramientas y sitios web.

La documentación entregada deberá incluir guías rápidas que faciliten las tareas diarias más comunes (administración de los diferentes contenidos, etc.).

Todos los entregables dirigidos a personas usuarias deberán ser bilingües (euskera y en castellano) y hacer un uso del lenguaje inclusivo no sexista.

4.9. 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 DSGVO recogidas en el Anexo 1: Normas de seguridad relativas a los sistemas de información.

4.10. Documentación no sexista

Toda la documentación, publicidad, imagen o material que se genere con motivo de la ejecución del contrato, la empresa o entidad adjudicatario 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.

4.11. 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 la DGTSI 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 de la DGTSI.

4.12. Lugar de ejecución del contrato.

La prestación del servicio se realizará en la empresa adjudicataria, pero con presencias puntuales en las oficinas de la DGTSI, en la sede de Erandio, por requisitos del proyecto en la realización de tareas concretas que así lo requieran.

5. DOCUMENTOS ANEXOS

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

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

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

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

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

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

1 Acceso y protección de datos

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

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

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

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

(1) *Normativa: Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Directiva (UE) 2016/680 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.*

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

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

2 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.