EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA

Administrazio eta Zerbitzuen Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak udeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD

Viceconsejería de Administración y Servicios
Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

MIGRACIÓN DEL PORTAL GURENET

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Larrauri Mendotxe bidea, 18 – 48950 ERANDIO (Bizkaia)

Tel. 94 607 80 00 – Fax 94 607 83 02

TABLA DE CONTENIDOS

Página

1. ANTECEDENTES Y OBJETO DEL PLIEGO 3

2. ALCANCE DEL CONTRATO. 4

2.1 LOTE 1: CREACIÓN DE SITES Y MIGRACIÓN DE CONTENIDOS 4

2.2 LOTE 2: MIGRACIÓN DE APLICACIONES 5

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS 6

3.1. LOTE 1: CREACIÓN DE SITES Y MIGRACIÓN DE CONTENIDOS 6

3.2. LOTE 2: MIGRACIÓN DE APLICACIONES 13

3.3. CONSIDERACIONES GENERALES 55

4. EJECUCIÓN DEL CONTRATO 58

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 58

4.2. ENTORNO TECNOLÓGICO 58

4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 60

4.4. GESTIÓN DE LA CALIDAD 61

4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 64

4.6. REGISTROS, NOTIFICACIONES E INVENTARIOS 64

4.7. LUGAR DE EJECUCIÓN DEL CONTRATO 65

5. DOCUMENTOS ANEXOS 66

5.1. ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 66

1. ANTECEDENTES Y OBJETO DEL PLIEGO

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, en adelante DGTSI, es la encargada de prestar servicios informáticos y de comunicaciones al Departamento de Seguridad del Gobierno Vasco (DSGV).

Con el fin de mejorar los servicios prestados, se ha dado comienzo a una serie de iniciativas, entre las que se encuetra 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.

Para poder continuar con el proceso de migración se desea empezar con la intranet coorporartiva, abordando ésta de forma paulatina. De acuerdo con estas necesidades se determinan las condiciones generales y particulares a las que debe ajustarse este proceso de migración, que constituyen la base para la petición de ofertas.

El objeto de este expediente es la contratación de los servicios para la migración, reingeniería y evolución tecnológica de los aplicativos seleccionados, contenidos y servicios de la intranet corporativa, así como los servicios y flujos de integración entre aplicaciones especificados en los apartados siguientes.

El presente pliego de prescripciones técnicas (P.P.T.) tiene como finalidad determinar el alcance de la prestación del servicio a realizar, así como las características generales y particulares y condiciones de ejecución a las que deben ajustarse el servicio solicitado.

2. ALCANCE DEL CONTRATO.

El presente expediente tiene por objeto la contratación de las tareas de análisis, diseño, construcción e implantación de la migración y reingeniería de las capas de presentación, integración y negocio (incluyendo las aplicaciones, servicios e integraciones en el entorno de la intranet corporativa, denominada Gurenet). Se debe garantizar así mismo que en este proceso de migración no se produce pérdida de funcionalidad ni de rendimiento.

Se trata de migrar la funcionalidad recogida en la intranet corporativa que se ejecuta bajo los productos IBM WebSphere Portal Server para la parte de presentación; IBM Web Content Manager para la gestión de contenidos; y por último IBM WebSphere Application Server como servidores en la parte de negocio, a la nueva infraestructura Liferay DXP y servidores de negocio WebLogic.

Es requisito llevar a cabo una reingeniería de las aplicaciones con el fin de proceder, así mismo, a su renovación tecnología y que se optimice y mejore el código implantado, ajustándose a los nuevos requerimientos tanto de seguridad como de calidad.

La contratación se llevará a cabo en los siguientes lotes:

- Lote 1: Creación de sites y migración de contenidos
- Lote 2: Migración de aplicaciones

2.1 Lote 1: creación de sites y migración de contenidos

Este lote debe dar respuesta a los siguientes requisitos con el fin de conseguir la migración de los contenidos actualmente existentes manteniendo la seguridad asociada a los mismos, así como determinadas funcionalidades ligadas a la gestión de determinados contenidos.

Los requisitos básicos a satisfacer son los siguientes:

- Creación de sitios web (incluyendo tema, jerarquía de páginas, etc.) para las diferentes áreas funcionales de la DGSV, así como para los equipos de trabajo que por sus características requieran de un sitio web dedicado en el producto Liferay DXP.
- Creación de las estructuras, plantillas de visualización, ADTs, flujos de publicación, etc., necesarias en la nueva intranet.
- Prototipado de los sitios para validación.

- Proceso para la migración de los contenidos actuales a la ubicación más apropiada de la nueva intranet, incluyendo metadatos, documentos asociados, flujos de trabajo, etc., equivalentes a los ya existentes en Gurenet
- Gestión de la seguridad a contenidos y documentos, tanto en el proceso de migración como en mantenimiento posterior que realizarán usuarios/as una vez haya finalizado la migración
- Mejora del sistema de auditoría de acciones ofrecido de serie por el producto Liferay DXP
- Incorporación de un buscador general de contenidos en la intranet y específico por site
- Proporcionar funcionalidades adicionales en la gestión de determinados contenidos, como puede ser la inclusión de marca de agua, visualizadores adicionales, etc.

2.2 Lote 2: migración de aplicaciones

Este lote contempla las tareas necesarias para llevar a cabo la migración de las aplicaciones identificadas en esta primera fase. Entre los trabajos a realizar se detallan los siguientes:

- migración de la capa de presentación (13 aplicaciones afectadas)
- modificación de la capa de presentación (4 aplicaciones afectadas)
- migración de la capa de negocio (17 aplicaciones afectadas)
- migración de la capa de integración (4 servicios identificados)

En ambos lotes, antes de abordar su desarrollo, la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos deberá aprobar la propuesta de trabajo presentada por la empresa adjudicataria con la planificación de los trabajos aportada a los requisitos planteados en el presente PBT.

Las empresas licitadoras podrán presentar ofertas por uno o más lotes.

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS

3.1. Lote 1: creación de sites y migración de contenidos

3.1.1 Sitios web

La actual intranet corporativa está compuesta por un único sitio web común a todas las personas usuarias. La nueva intranet no mantendrá este enfoque monolítico y se dividirá en varios sitios web, existiendo un único sitio de carácter general para todas las personas que acceden a la intranet y varios sitios específicos para aquéllas que tengan alguna característica común (como puede ser la organización a la que pertenecen). Así mismo, será posible, definir "subsitios" dedicados a equipos de trabajo o grupos de personas con requisitos especiales.

Cada uno de los sitios creados tendrá su propia identidad: logotipos, tema, paleta de colores, etc., aunque podrán compartir una línea de diseño común que refleje su pertenencia al Departamento. Los temas creados deberán ser "responsive", es decir, que su visualización y apariencia deberá adaptarse de forma automática, ser usable y accesible en el navegador o dispositivo utilizado para su acceso (PCs de escritorio, portátiles, tablets o dispositivos móviles, etc.). Además, los temas deberán desarrollarse teniendo en cuenta que las aplicaciones que acabarán albergando son típicas de una intranet (intensivas en datos con formularios, tablas, listados, etc.).

Todos los sitios y subsitios deberán ser bilingües (euskera y castellano), 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.

3.1.2 Migración de contenidos

Todos los contenidos de los diferentes sitios web de la intranet son privados, es decir, solamente los podrán crear y actualizar las personas que sean administradoras de los mismos. Podrán existir diferentes roles administradores dentro de un mismo site y se deberá garantizar que cada persona solo pueda consultar o manipular aquellos contenidos a los que esté autorizada, pero que no podrá ni consultar ni manipular los administrados por los otros roles administradores. Así mismo, los contenidos a visualizar dependerán del rol asignado a cada una de las personas que vayan a acceder.

En la intranet actual, los contenidos se encuentran repartidos en varias bibliotecas. Algunas de ellas solo incluyen contenidos generados por un solo grupo determinado de personas autorizadas, pero en otros casos albergan contenidos de diferentes naturalezas generados por grupos de diferentes Direcciones. Durante la migración, se deberá analizar y proponer el sistema más adecuado de organizar estos contenidos. El proceso de migración deberá leer el contenido de todas las bibliotecas y grabarlo en la ubicación más adecuada de la nueva intranet, y deberá tener, como mínimo, las siguientes características:

- la migración deberá ejecutarse de forma desatendida y por personal ajeno al equipo de desarrollo
- la migración deberá estar diseñada teniendo en cuenta que puede ser ejecutada más de una vez
- el proceso deberá generar un informe o registro con el resultado de la migración
- el código del o de los procesos de migración, así como de cualquiera de sus elementos auxiliares se considera un entregable más del proyecto
- el propio contenido web bilingüe y sus metadatos asociados (título, fecha de creación, publicación, estado, etc.), preservando sus valores originales
- el histórico de versiones o cambios en cada uno de los contenidos migrados
- la definición de estructuras necesarias para cada contenido
- las plantillas de visualización y ADTs necesarios para su correcta visualización
- taxonomía o vocabularios y categorías asociadas a cada contenido web, si aplica
- documentos y ficheros adjuntos

- flujos de trabajo o publicación
- la ubicación de todos los elementos previos en el lugar más apropiado en función de la seguridad y control de acceso exigido
- permisos de acceso y elementos relacionados para todos los contenidos, sean del tipo que sean, tratados en el proceso de migración.

La preservación de los permisos de acceso a contenidos, al pasar de un único sitio web (Gurenet) a varios sitios web se considera crítica, tanto por motivos de seguridad como de difusión. Por ejemplo, existen casos en los que los contenidos que deben mostrarse en varios sitios web (noticias, comunicaciones, normativas o directrices, etc.). Así mismo, la mayoría de contenidos deben tener un acceso limitado y controlado.

Es necesario que exista la posibilidad de que las personas usuarias de los sitios web puedan suscribirse y recibir notificaciones ante cambios en determinados contenidos de su elección; por ejemplo, recibir un correo electrónico que avise de la publicación de una nueva noticia, una norma, un aviso, etc. Se requiere también que el usuario sea capaz de indicar si lo estima necesario el correo electrónico de destino para las notificaciones.

Se han identificado dieciséis grupos de bibliotecas a migrar, aunque el dato final se determinará en la etapa de análisis del proyecto.

3.1.3 Migración de documentos a SharePoint

El proceso de migración incluye un caso especial que requerirá la migración de documentos de diferentes tipos albergados en una biblioteca al producto Microsoft SharePoint.

El proceso de migración de estos contenidos deberá mantener los permisos de acceso existentes y al igual que el resto de procesos de migración, deberá poderse ejecutar de forma desatendida por personal ajeno y cumplir con el resto de requisitos especificados anteriormente.

3.1.4 Seguridad en los contenidos

Aunque puede haber contenidos de carácter semipúblico (visible por todas las personas y autorizadas en el sitio web) como avisos o comunicaciones, una parte importante solamente estará disponible para los individuos que pertenezcan a grupos concretos.

La naturaleza de muchos de estos contenidos exige un estricto control de acceso de varios niveles, que van desde el control completo sobre un contenido a limitar incluso la posibilidad de conocer su existencia.

Por ejemplo, en la pantalla de inicio de un sitio web suele haber un publicador de contenidos que muestre noticias para todas las personas usuarias identificadas y otras noticias cuya visualización esté limitada a grupos concretos. En el caso de personas con la capacidad de crear contenidos web, solo deben tener acceso (incluso visual) a contenidos autorizados. Esto es aplicable también a los documentos.

En el caso de personas que dispongan de permisos administrativos como editores o revisores de contenidos, aquéllas solamente deberán tener acceso (incluso visual) a sus carpetas y contenidos.

La propuesta deberá incluir no solamente la seguridad en el momento de la migración, sino que deberá incluir la seguridad en las acciones que los y las usuarias realizarán en sus labores diarias de creación, edición, etc., de contenidos y documentos una vez finalizada la migración; por ejemplo, que nuevos contenidos hereden los permisos apropiados. Además, se deberá tener en cuenta que las personas usuarias finales no tendrán perfil técnico y que el control de seguridad no debe interferir en su trabajo diario.

3.1.5 Auditoría de acciones

Liferay DXP incluye un módulo de auditoría que registra acciones básicas sobre elementos: visualización de páginas, edición de contenidos y documentos, etc. Este nivel de auditoría es insuficiente para las necesidades del DSGV.

En concreto, es necesario tener la posibilidad de que ciertos grupos autorizados puedan conocer con precisión qué acciones se realizan, como, por ejemplo:

- creación, edición, copia, borrado, expiración, etc., de contenidos de cualquier tipo
- movimiento de contenidos de cualquier tipo entre carpetas
- creación, renombrado y borrado de carpeta
- descarga de documentos
- cambios en los permisos de acceso a contenidos de cualquier tipo

En resumen, se desea tener una trazabilidad lo más completa posible de las acciones realizadas por cualquier persona, incluyendo las realizadas en procesos programados o ejecutados de forma automática como la publicación o expiración de contenidos, tanto en los sitios web creados durante el proceso de migración como en los nuevos sitios web que puedan crearse en un futuro.

3.1.6 Funcionalidades que debe incluir la gestión/visualización de contenidos.

Actualmente y con el fin de facilitar la administración a los y las creadoras de contenidos, existen una serie de funcionalidades para la creación y el acceso a los contenidos del portal. Sin embargo, como norma general, el objetivo en esta migración es simplificar este enfoque, utilizando al máximo posible las funcionalidades que ofrece el producto Liferay DXP, como son los flujos de aprobación, acciones personalizadas tras la publicación o actualización de un contenido como, por ejemplo, el envío de correos electrónicos, generación de newsletters, etc.; si bien se deben cumplir los requisitos de seguridad y auditoria.

No obstante, hay algunos desarrollos que se deberán tener en cuenta en la migración como pueden ser la inclusión de marca de agua en los documentos PDF, el buscador de grupos o el selector de categorías.

Por consideraciones de seguridad y trazabilidad habrá documentos en formato PDF para los que no deberá ser posible su descarga directa, es decir, que no se podrá descargar la versión original del documento PDF sino una copia personalizada y única que identifique la persona que está accediendo o descargando el documento y el momento en el que realiza la acción.

Por ejemplo, que en el momento de la descarga de determinados documentos se deberá añadir marcas de agua a todas sus páginas con datos que identifiquen la persona que ha accedido al mismo, y metadatos no visibles como la fecha y hora de la descarga, así como la modificación de propiedades del documento PDF para indicar que no puede ser impreso, que no se puede copiar su contenido, etc. En documentos que se visualicen de forma embebida dentro de las aplicaciones se podrá limitar las opciones de descarga, impresión, envío, etc.

Así mismo, se deberá disponer de un componente accesible desde la gestión de contenidos que proporcione a la persona administradora del mismo, la posibilidad de seleccionar los colectivos que tendrán acceso a cada contenido.

Este componente deberá mostrar una pantalla en donde aparezcan:

- Criterios de búsqueda: opción para poder buscar por roles. Se podrá introducir:
  - nombre del rol
  - descripción del rol
- Lista de resultados: apartado donde aparecerán los roles que cumplan con los criterios de búsqueda. En este apartado se seleccionarán los roles que se quieran asignar al contenido.

Una vez seleccionados los roles, se deberá asignar dichos permisos al contenido. Solo se podrán visualizar los roles a los que la persona usuaria tiene acceso.

Por último, deberá diseñarse un selector de categorías que permita mejorar la usabilidad del producto.

3.1.7 Buscador de contenidos

Todos los sites incorporarán un buscador que permitirá, respetando las restricciones de seguridad de acceso, realizar búsquedas que devuelvan resultados con contenidos presentes en dicho site.

Además, se requiere la funcionalidad de un buscador de contenidos global que, respetando las mismas restricciones de seguridad de acceso, permita realizar búsquedas que devuelvan resultados con contenidos presentes en cualquier site de la intranet del DSGV.

Por ejemplo, si el perfil de una persona usuaria le habilita el acceso a dos sites, se desea que al realizar una búsqueda los resultados obtenidos incluyan los contenidos de ambos sites a los que la persona usuaria tenga acceso, independientemente de la posible relación de jerarquía que pueda haber entre los sites.

En cualquiera de los casos, los resultados no deberán mostrar información asociada a las personas creadoras de los contenidos.

El aplicativo deberá encontrar coincidencias tanto en los contenidos como en los documentos anexos.

Para permitir las búsquedas, las estructuras deberán estar configuradas por defecto para habilitar su búsqueda e indexación.

Los filtros de búsqueda deberán contemplar al menos las siguientes condiciones:

- Búsqueda por texto libre
- Búsquedas por categoría

3.1.8 Tema de los sites

Los temas para la apariencia visual de los sites objeto de la migración deberán incluir, además de los ajustes necesarios para la correcta visualización de su site, los estilos necesarios para que las aplicaciones a migrar en el lote “2” se integren en la apariencia visual del site. Es decir, los temas deberán definir todos los estilos visuales tanto para el sitio web como para las aplicaciones que se vayan a desplegar (ver apartado “Entorno tecnológico” para conocer las tecnologías y frameworks de presentación).

Dado que los dos lotes que componen este documento se desarrollarán en paralelo, la disponibilidad temprana de un tema que defina la apariencia visual tanto de sites como de aplicaciones es requisito necesario para no bloquear la ejecución del lote “2”. Este tema inicial podrá refinarse y depurarse a medida que avance la ejecución de ambos lotes con el feedback recibido durante la ejecución del lote “2”.

3.2. Lote 2: migración de aplicaciones

3.2.1 Aspectos generales a todas las aplicaciones

El proceso de migración y reingeniería deberá cumplir los siguientes requisitos:

- adaptación y actualización de los desarrollos a la versión 8 del lenguaje de desarrollo Java;
- adaptación y actualización de los desarrollos portlet a la especificación Portlet 3.0 con el estándar Java Server Faces 2.2;
- adaptación y actualización de los desarrollos Java EE 1.3, 1.4, 5 y 6 a la especificación Java EE7;
- eliminación de la denominada “deuda técnica”;
- sustituir el uso de librerías internas como “BIDEA” y “OINARRI” por su equivalente más actual “GIDA”;
- 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;
- simplificar la arquitectura y mantenimiento de las aplicaciones, ubicando las aplicaciones dirigidas a varios colectivos en un único site que identificará la DGTSI y al que accederán los distintos colectivos y donde se les presentará, en función de su perfil, la aplicación con las funcionalidades requeridas;
- migración de informes generados con Apache FOP o JasperReports, que deberán adaptarse a la versión más reciente de JasperReports o hacer uso de IberDok, en función de las necesidades funcionales.

3.2.2 Migración de la capa de presentación

Los aplicativos web de la actual intranet del Departamento están desarrollados con las siguientes tecnologías: IBM Portlet de tipo básico o usando el Struts Portlet Framework; Portlet 1.0 de tipo básico o usando el Struts Portlet Framework; Portlets 2.0 + JSF 2.0 usando Primefaces 6.1; servlets, etc. Dichos aplicativos se integran con las actuales capas de negocio e integración a través de peticiones RMI, SOAP y REST, propagando la identidad de la persona logada en el portal.

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

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

3.2.3 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

3.2.4 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

3.2.5 Migración de datos

Las aplicaciones del Departamento persisten sus datos en diferentes bases de datos:

- DB2 z/OS
- DB2 LUW
- Oracle RAC
- SQL Server

En las aplicaciones seleccionadas, no se ha visto la necesidad de migración de los datos del SGBD actual donde residen. Si bien, el Departamento de Seguridad está inmerso en un proyecto de migración del actual sistema Host, denominado zBerritu, en el cual la actual BBDD DB2 z/OS se migrará a SQL Server, por lo que a lo largo de este proyecto la BBDD de los aplicativos, que tengan dependencias con aplicativos del mainframe y usen DB2 z/OS, podrá cambiar y en la migración deberán adaptarse al nuevo SGBD.

Cualquier modificación sobre la estructura de las tablas deberá ser comunicada para su autorización de cara a evaluar su impacto sobre los procesos de DataWarehouse existentes.

3.2.6 Aplicaciones a migrar

Las aplicaciones a migrar se han clasificado del siguiente modo:

GRUPO APLICACIÓN	Agrupación	APLICACIÓN
Aplicaciones Policías Locales	Fase 1	A30 LSC
	Fase 2	A25 Equipo Humano A26 Talkies A27 Servicio de Auditoría A28 Mensajes y Consultas
	Fase 3	A29 Evidencias A47 Registro Policías Locales B89 RVATE
Aplicaciones Tráfico	Fase 1	A46 Documentación Sanciones B52 Radares
	Fase 2	A91 Vialidad Invernal A91 Cámaras de Tráfico
	Fase 3	A32 Registros DGT A36 Permiso por Puntos
Aplicaciones DSGV	Fase 1	B61 Embajadas y consulados B67 Dudatan
Aplicaciones Policiales	Fase 1	A20 Informes Fotográficos

A continuación se describe cada una de ellas ordenada por su código de aplicación.

3.2.6.1. A20 – Informes Fotográficos

Descripción funcional

La presente aplicación tiene como objetivo principal la creación de una base de datos de fotografías, asociadas a los informes técnicos y su mantenimiento. Toda esta información fotográfica (en formato digital) generada con motivo de los atestados gestionados por la Ertzaintza está dirigida a formar parte de los informes enviados a los juzgados.

La aplicación cuenta con dos partes:

- Administración: En este apartado, la persona con perfil administrador encuentra la funcionalidad para el mantenimiento de los siguientes datos estáticos de la aplicación:
    - Entidades: Referente a los tipos de referencias policiales del Sistema de Información Policial (Atestados, Inspecciones Oculares, Denuncias…).

  - Plantillas: Plantillas de Informes fotográficos.
  - Grupos de investigación: Grupos de investigación pertenecientes a cada una de las unidades de la Ertzaintza.
- Informes: En este apartado se dispone de la funcionalidad para crear o modificar (añadir fotografías, actualizar datos, etcétera), de un informe técnico. También tiene como finalidad la consulta del informe (para ver sus fotografías, imprimirlas…). Dentro de este apartado, la persona usuaria puede:
  - Realizar Informes: esta opción muestra el buscador de Informes en elaboración y da entrada al módulo de creación y mantenimiento de Informes Técnicos.
  - Consulta de Informes Publicados: esta opción muestra el buscador de Informes publicados.

Los informes fotográficos pueden estar en cuatro estados distintos que definen el flujo de trabajo y ciclo de vida de éstos:

- Borrador. Es el primer estado por el que pasa un informe. Sólo es obligatorio el número de referencia y se utiliza para asociar las fotografías descargadas.
- En elaboración. Cuando a un informe se le incluyen fotografías o se añade alguna fotografía adicional, pasa al estado de elaboración.
- Publicado. Al publicarse un informe, pasa al estado publicado.
- Despublicado. Cuando se despublica, pasa a estado “En elaboración” y se crea un informe en estado “despublicado” que sirve de referencia.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	Oracle 19c
Integraciones	Integración con Servicio Horizontal NORA

	Integración con el Servicio Horizontal Kudok (API de integración con el Gestor documental corporativo) Integración con el Servicio Horizontal Registro Auditoría. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA. Generación y Edición de documentos con ASPOSE. Esta integración deberá ser sustituida por Iberdok para la generación de documentos. Integración con z/OS Host mediante colas MQ Series. Esta integración deberá ser trasladada al ESB corporativo Oracle Service Bus 12c.
Seguridad	Acceso restringido. Existen 5 roles de seguridad. La administración de esta aplicación puede ser realizada por los usuarios
LOPD	Todas las acciones de alta/modificación/baja/consulta sobre los registros de informes fotográficos son y deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.2.6.2. A25 – Equipo Humano

Descripción funcional

Aplicación que permite crear y editar datos estadísticos sobre los diferentes equipos que forman las policías locales. Incluye tres acciones: consulta, inserción y modificación de datos estadísticos de siete categorías para un determinado municipio y en un año:

- por cometido;
- por sexo;

- por origen;
- por año de nacimiento;
- por nivel de estudios;
- por categoría; y
- por escala.

Esta aplicación incluye además un proceso batch invocado por la aplicación Control-M que se encarga de realizar una carga de los datos registrados en esta aplicación a un esquema de base de datos utilizado para tareas de DataWareHouse.

Tecnologías e integraciones

Tecnologías negocio	Java 1.5, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.5, Struts Framework Portlet, IBM Portlet
Persistencia	Oracle 19c
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP: director, encargado y auxiliar de DCPL. Utiliza un único perfil de seguridad.

3.2.6.3. A26 – Talkies

Descripción funcional

Aplicación que gestiona la asignación de talkies a los diferentes turnos de trabajo de los policías locales en cada comisaría. Incluye la siguiente funcionalidad:

- información sobre los horarios de trabajo de cada centro policial
- composición y ratificación de turnos
- consulta de agentes conectados
- relación de talkies asignados a cada agente dentro de un turno de trabajo.

Funcionalmente trabaja con tres roles de usuario: jefatura, agente e inspección de la Policía Local. Las personas que tengan el rol de jefatura pueden administrar y ratificar turnos, grupos de trabajo y realizar las asignaciones. Las personas que tengan el rol de agente podrán realizar consultas sobre sus turnos, consultar qué agentes tienen los terminales conectados y las asignaciones de talkies. Existe un rol adicional de tipo “Administrador” con acceso completo a la aplicación.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales a través de la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para los usuarios del Departamento de Seguridad añadiendo los perfiles de usuario que sean necesarios. Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto y consumido por la aplicación en proceso de migración mantenga su funcionamiento.

No tiene integraciones con aplicaciones o servicios externos, aunque publica un servicio de auditoría que se utiliza desde otros proyectos, que deberá integrarse en el servicio horizontal actual de autoditoría.

Tecnologías e integraciones

Tecnologías negocio	Java 1.5, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.8, Portlet 2.0, PrimeFaces 8.0 (Liferay)
Persistencia	Oracle 19c DB2 Host
Integraciones	Integración con el Servicio Horizontal “Kudok” de Gestión Documental

	Integración con el Servicio Horizontal Registro Auditoría de OINARRI. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA. Así mismo, se deberá revisar su uso, con el fin de que todas las acciones queden correctamente auditadas Consume las tablas de DB2 Host de maestro de terminales
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP: un colectivo compuesto por cada una de las comisarías de policías locales con acceso a la aplicación, y otro colectivo compuesto por auxiliar, encargado, y director de la Dirección de Coordinación de Policías Locales.
LOPD	Todas las acciones realizadas deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.2.6.4. A27 – Servicio de Auditoría

Descripción funcional

Aplicación para el registro de trazas y rastros de auditoría. La aplicación diferencia entre trazas o *logs* de depuración, que registran quién, qué, cuándo, dónde y por qué un evento ocurre en una aplicación o componente; y rastros de auditoría, que incluyen información necesaria para realizar la auditoria de accesos y modificaciones de datos en una aplicación o componente.

Está compuesto por dos módulos diferenciados: uno en la capa de presentación y otro en la capa de negocio.

El módulo de presentación aplica un control de acceso de grano fino a los datos de aplicaciones auditadas. Facilita la tarea de búsqueda y filtrado de los datos registrados y permite la generación de documentos en formato PDF o Excel con el resultado de las consultas realizadas.

El módulo de negocio, además de las operaciones necesarias para las consultas realizadas desde la capa de presentación, publica un servicio web SOAP en el OSB para ser consumido con afección mínima por parte de las aplicaciones consumidoras de este servicio, y dispone de estrategias para ofrecer una garantía de servicio para su recuperación ante fallos de diverso tipo, intentando minimizar al máximo los posibles problemas derivados de fallos, como pérdida de datos, indisponibilidad del servicio, etc. Estas estrategias de garantía de servicio deberán mantenerse en la aplicación resultante de los procesos de migración y reingeniería.

El servicio web SOAP publicado en el OSB12 deberá evolucionar para integrarse con el proyecto una vez migrado manteniendo el API expuesto y toda su funcionalidad.

El servicio de auditoría es uno de los servicios horizontales del Departamento, y por ello, uno de los más críticos.

Funcionalmente la aplicación define cuatro roles: auditor administrador, con el que se podrá consultar los rastros de todas las aplicaciones configuradas en el sistema; auditor SIP, con el que se podrán consultar los rastros de las aplicaciones policiales; auditor PPLL, con el que se podrán consultar los rastros de las aplicaciones para policías locales; y auditor aplicación, con el que se podrán consultar los rastros de una o varias aplicaciones específicas para las que se haya concedido autorización.

Tecnologías e integraciones

Tecnologías negocio	Java 1.5, J2EE 1.3, EJB 2.1
Tecnologías de presentación	Java 1.5, Struts Framework Portlet, IBM Portlet
Persistencia	Oracle 19c
Integraciones	Publica un servicio web SOAP en el OSB12 Incluye un proceso batch ejecutado por Control-M para la carga de registros de auditoría.

	La generación de documentos PDF utiliza una versión antigua de las librerías iText y Apache FOP para la generación de documentos en formato PDF. La generación de documentos PDF deberá actualizarse para utilizar JasperReports o LibrePDF. La generación de documentos Excel se realiza manipulando documentos XML y utilizando XSL. La generación de documentos Excel deberá actualizarse para utilizar librerías actuales como Apache POI.
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP. Funcionalmente se definen dos perfiles: jefe de policía local, que tendrá acceso a los rastros de su centro y personal del Área de Coordinación de Policías Locales, que tendrá acceso a los datos de todos los centros de policía local.
LOPD	Todas las acciones de consulta realizadas se deberán seguir registrando en el módulo de auditoría. Deberá garantizarse que la traza de auditoría se guarda correctamente, por lo que se valorará positivamente toda mejora que aporte una mayor garantía en la prestación de esta servicio con garantía.

3.2.6.5. A28 – Mensajes y consultas

Descripción funcional

Aplicación con dos módulos a migrar: mensajes y consulta de antecedentes. Esta aplicación incluye un tercer módulo llamado “Avisos” que queda fuera del alcance de este pliego.

“Consulta” consume operaciones de negocio expuestas por varios proyectos del Departamento para lanzar consultas sobre personas y vehículos. Estas consultas recopilan datos de la DGT y a aplicaciones internas del Departamento, y se muestran los resultados obtenidos de forma agregada, pudiéndose generar de forma opcional un documento PDF con el resultado de estas consultas. Cualquier individuo con acceso a la aplicación podrá realizar consultas.

“Mensajes” ofrece un servicio de mensajería entre la Dirección de Coordinación y las Policías Locales. Realiza la gestión y control de los mensajes leídos y pendientes de leer por parte de ambas partes, así como de los acuses de recibo.

Tiene las siguientes funcionalidades: creación de nuevos mensajes, administración de mensajes recibidos y de mensajes enviados. Los mensajes podrán dirigirse a tres grupos de usuarios de la DCPL, a uno o más Territorios Históricos, o a uno o más municipios. También es posible el envío de mensajes directamente a personas.

Además de los tres roles habituales en las aplicaciones de Policías Locales (jefatura, inspección y agentes), “Mensajes” incluye los siguientes roles para la comunicación con DCPL: auxiliar, encargado y dirección de la DCPL.

“Mensajes” define además un rol adicional “Administrador” con acceso completo.

Este proyecto consume el servicio de auditoría publicado por A26, que deberá ser cambiado.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales desde la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para los usuarios del Departamento de Seguridad añadiendo los perfiles de usuario que sean necesarios. Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto y consumido por la aplicación en proceso de migración mantenga su funcionamiento.

Tecnologías e integraciones

Tecnologías negocio	Java 1.5, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.8, Portlet 2.0, PrimeFaces 8.0 (Liferay)
Persistencia	Oracle 19c
Integraciones	Integración con el Servicio Horizontal “Kudok” de Gestión Documental Integración con el servicio de auditoría publicado por A26. Esta integración deberá cambiarse y el nuevo aplicativo se integrará con el Servicio Horizontal de auditoría publicado por la librería GIDA. Así mismo, se deberá revisar su uso. Utiliza versiones antiguas de Apache FOP e iText para la generación de documentos PDF, que deberá actualizarse para utilizar JasperReports o LibrePDF Consume operaciones expuestas por varias aplicaciones o servicios Departamento (se han identificado 3): Esta integración se realiza consumiendo operaciones mediante el estándar RMI. Estas operaciones deberán consumirse como servicios web SOAP, aplicándose las adaptaciones necesarias a estas aplicaciones externas

Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP. "Consultas" permite el acceso a los usuarios de las comisarías de policías locales. "Mensajes" permite el acceso a usuarios que tengan asignado uno de los tres roles autorizados de Policías Locales, o uno de los tres roles autorizados de DCPL.
LOPD	Todas las acciones realizadas deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.2.6.6. A29 – Evidencias

Descripción funcional

Proporciona un cauce de comunicación entre las Policías Locales y la unidad de policía científica de la Ertzaintza, en el marco de las investigaciones criminales con evidencias:

- funcionalidades tendentes a facilitar la comunicación entre la policía científica de la Ertzaintza y los investigadores de las policías locales de manera que permita:
  - la identificación de las evidencias y su procedencia
  - la documentación del envío y-devolución de las evidencias municipales (cadena de custodia de las mismas)
  - la consulta del grado de evolución de los exámenes que están siendo llevados a cabo por parte de la unidad de policía científica (estado de los estudios en cada momento)
  - la publicación de los resultados obtenidos.

La aplicación está compuesta por los siguientes módulos principales:

- gestión de solicitudes
- maestros de evidencias, descartes, hechos e implicados / personas descartadas
- autorizaciones

La gestión de solicitudes permite la creación, modificación, eliminado y formalización de consultas de solicitudes de estudio pericial sobre un determinado hecho ya existente o uno nuevo. Una solicitud podrá tener asociación además de con un hecho, con evidencias, estudios de diferentes tipos asociados a un conjunto propio de evidencias e implicados, personas descartadas y personas implicadas.

La respuesta obtenida desde la Ertzaintza para cada solicitud podrá incluir el informe pericial solicitado, una lista variable de subcasos creados para la evaluación de las evidencias de la solicitud y referencias que forman cada subcaso, que a su vez podrán incluir evidencias y personas relacionadas.

Por último, también se permite la generación de documentos PDF de una solicitud una vez formalizada.

Los maestros de evidencias, descartes, hechos e implicados / personas descartadas permiten la gestión de estas entidades, que irán asociadas a una solicitud.

La aplicación incluye también un servicio web SOAP expuesto a través del producto Oracle OSB12 y que se consume desde terceras aplicaciones, que no forma parte del alcance de esta migración.

Funcionalmente trabaja con tres roles de usuario: jefatura, agente e inspección de la Policía Local. Estos tres roles definen dos perfiles diferenciados: uno de ellos se asocia a los agentes de Policías Locales, y tendrá menos acciones disponibles que el segundo perfil, asociado a jefatura e inspección de Policías Locales.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales desde la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para los usuarios del Departamento de Seguridad añadiendo los perfiles de usuario que sean necesarios. Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto y consumido por la aplicación en proceso de migración mantenga su funcionamiento.

Tecnologías e integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.8, Portlet 2.0, PrimeFaces 8.0 (Liferay)
Persistencia	Oracle 19c
Integraciones	Integración con el Servicio Horizontal "Kudok" de Gestión Documental Integración con el servicio de auditoría publicado por A26. Esta integración deberá cambiarse en el nuevo aplicativo para que se integre con el Servicio Horizontal de auditoría de GIDA. Así mismo deberá revisarse el alcance de su uso.
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP: jefatura, inspección y agentes de Policía Local.
LOPD	Todas las acciones realizadas deberán ser registradas mediante el Servicio Horizontal de Auditoría.

3.2.6.7. A30 – Ley de Seguridad Ciudadana

La aplicación facilita la introducción y envío al Departamento de Seguridad por parte de las Policías Locales de informes de denuncias por infracciones de la Ley Orgánica sobre Protección de la Seguridad Ciudadana (LSC). Además del envío, la aplicación permite a las Policías Locales la consulta de su estado para conocer las resoluciones del Departamento a estos informes, es decir, si ha decidido sobre su incoación o no:

a) informes no incoados con los motivos aducidos para la no incoación

b) informes incoados con resolución firme y las sanciones a las denuncias reflejadas en estos informes.

Al crear un informe, en función del tipo de infracción se deberán completar más o menos bloques de datos en el formulario de creación: analíticas, documentos anexos, estupefacientes, informes, personas, vehículos y objetos incautados. Una vez creado el informe se envía al SIP para su evaluación. Una vez disponible la resolución se actualiza el estado del informe y se podrán generar documentos con notificaciones de sanciones.

Se podrán obtener listados de informes de LSC en formato PDF.

Funcionalmente la aplicación define tres roles de usuario: jefe, inspección, agente y auxiliar de Policía Local.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales desde la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para los usuarios del Departamento de Seguridad añadiendo los perfiles de usuario que sean necesarios. Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto y consumido por la aplicación en proceso de migración mantenga su funcionamiento.

Tecnologías e integraciones

Tecnologías negocio	Java 1.6, J2EE 1.4, EJB 2.1 Java 1.7, Java EE6, EJB 3.1
Tecnologías de presentación	Java 1.8, Portlet 2.0, PrimeFaces 8.0 (Liferay)
Persistencia	Oracle 19c Consulta datos de DB2 HOST
Integraciones	Integración con el Servicio Horizontal “Kudok” de Gestión Documental Integración con el servicio de auditoría publicado por A26. El nuevo aplicativo se deberá integrar con el Servicio Horizontal de auditoría de GIDA. Así como revisar el alcance de su uso.

	Añadir un nuevo rol de usuario para que la Dirección de Coordinación de Policías Locales tenga acceso a la aplicación. Integración con el entorno IBM Host mediante colas JMS/MQ. Esta integración deberá ser trasladada al ESB corporativo Oracle Service Bus 12c. Incluye un proceso batch invocado por Control-M para la generación de documentos en formato PDF con notificaciones de sanciones. La construcción del documento se realiza utilizando librerías de otro proyecto (B27) para generar documentos PDF con la librería iText. La generación de documentos deberá actualizarse para generarse haciendo uso de JasperReports y/o la librería LibrePDF
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP: jefatura, inspección y agentes de Policía Local.
LOPD	Todas las acciones realizadas se deberán registrar en el módulo de auditoría.

3.2.6.8. A32 – Registros DGT

Descripción funcional

El sistema de Registros DGT se concibe como un sistema horizontal que ofrece a las aplicaciones departamentales servicios de consulta de antecedentes de personas y/o vehículos a través de los servicios web expuestos por la DGT (ATEX).

La capa de servicios ofrece a las aplicaciones distribuidas que así lo requieran servicios web horizontales expuestos sobre el ESB Oracle Service Bus 12c y servicios IBM ACE para consumo por aplicaciones HOST.

El sistema también cuenta con una aplicación web, accesible desde la intranet coorporativa, donde las personas tramitadoras de la Dirección de Tráfico o de la Ertzaintza pueden consultar antecedentes de personas y/o vehículos filtrados por datos del vehículo nacional/UE o datos del conductor (filiación, CIF/DNI). La aplicación web a partir del vehículo o conductor mostrado en pantalla permite generar informes basándose en librerías Velocity/FOP.

La aplicación se integra con el Sistema de Información Policial (SIP) por medio de colas MQ para notificar consultas realizadas por el personal policial sobre vehículos restringidos.

Otra funcionalidad web utilizada por aplicaciones del sistema centralizado HOST es un servlet el cual, a partir de la información cifrada pasada por parámetro, descifra su contenido en parámetros de consulta de un vehículo/conductor y devolverá a la aplicación cliente un pdf con el informe del elemento consultado

La aplicación cuenta con 4 perfiles diferentes. El primero se usa para determinar quién tiene acceso a la aplicación y los tres restantes los 3 tipos de consulta para los que se está autorizado:

- perfil de acceso a la aplicación
- perfil de acceso a los antecedentes de personas y los datos del conductor
- perfil de acceso a los antecedentes de vehículos nacionales
- perfil de acceso a los antecedentes de vehículos de la UE

Además de los servicios sobre los buses corporativos y la aplicación web, el sistema dispone de 3 procesamientos diferidos en Control-M para:

- recuperar a partir de un lote de base de datos nuevas solicitudes pendientes
- recuperar a partir de un lote de base de datos nuevas solicitudes fallidas
- procesar de vehículo/persona y un procesamiento que envía por correo consultas no procesadas.

El nuevo sistema horizontal a migrar deberá ofrecer en su conjunto las mismas funcionalidades actuales a aquellas aplicaciones departamentales que las demandan. Para ello la migración y reingeniería del siguiente sistema incluirá acometer las siguientes tareas de análisis y desarrollo:

a) migración de la aplicación web Registros DGT que permite a usuarios/as realizar las siguientes consultas:
   - antecedentes de personas
   - vehículos nacionales y de la UE
   - datos del conductor (filiación, CIF/DNI).

b) migración de los procesos de negocio encargados de la integración con los servicios web expuestos por la DGT (ATEX) utilizados por la aplicación web y los servicios expuestos en el ESB Oracle Service Bus 12c

c) migración del servlet que permita a las aplicaciones HOST visualizar un pdf con el informe del elemento consultado.

d) migración del actual servicio B57-SIP expuesto en IBM ACE para aplicaciones HOST del Sistema Información Policial al ESB Oracle Service Bus 12c

e) adaptación de los actuales servicios de Registro DGT de la capa de integración ESB Oracle Service Bus 12c para que se integren con los nuevos procesos de negocio.

f) adaptación de los actuales informes FOP a Jasper Report.

g) adaptación de los actuales procesos Batch de Control-M para invocar a los nuevos procesos de negocio.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet, SpringJDBC
Persistencia	DB2 Host

Integraciones	Servicio Web ATEX DGT Servicio horizontal de Auditoria de accesos. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA. Integración con el entorno IBM Host mediante colas JMS/MQ. Esta integración deberá ser trasladada al ESB corporativo Oracle Service Bus 12c. Servicio horizontal de correo Servlet expuesto a las aplicaciones HOST que tras la migración se generará con plantillas Jasper Report. 3 procesos Control-M
LOPD	La aplicación audita las peticiones realizadas hacia consultas ATEX.

3.2.6.9. A36 – Permiso por Puntos

Descripción funcional

La Dirección de Trafico cuenta con un Sistema de permiso por puntos (PPP) que proporciona un conjunto de aplicaciones y servicios relacionados con información del RCI (Registro de Conductores e Infractores) de la DGT. El sistema PPP de la Dirección de Tráfico del Gobierno Vasco se integra con el sistema centralizado de la DGT y nutre/consulta información centralizada en lo respectivo a:

- ✓ Consulta de saldo de puntos
- ✓ Envío de remesas RECEME
- ✓ Anotación de cursos organismos externos (ANCOREX)
- ✓ Cumplimiento de medidas reeducadoras

Entre las aplicaciones web y servicios que ofrece el sistema actual y que son objeto de la migración se encuentran las siguientes:

a) migración de la aplicación consulta de saldos en Gurenet para las oficinas territoriales de tráfico y de los procesos de negocio utilizados por la aplicación web.
b) adaptación del servicio Web de asignación/actualización de los datos de cursos e integración con ANCOREX/RECEME
c) adaptación de los procesos batch de envío/respuesta de remesas RECEME y anotación de cursos ANCOREX

En el proceso de migración las aplicaciones se ajustarán a las versiones más actuales que disponga la DGT para su integración.

El acceso a las distintas aplicaciones estará restringido por un conjunto de grupos LDAP que tienen acceso a portlets de Gurenet y que accederán según el caso a los recursos de la aplicación (ACL).

a) migración de la aplicación consulta de saldos en Gurenet

La aplicación web permite a personas tramitadoras de la Dirección de Tráfico realizar las siguientes consultas sobre información de la ciudadanía introduciendo su DNI:

- Puntos de la DGT. Se integrará con la operación de consulta de Saldo de Puntos del servicio Web de la DGT.
- Multas de la Dirección de Tráfico del Gobierno Vasco.
- Multas del registro de infractores de la DGT. Se integrará con la operación de consulta de Antecedentes del servicio Web de la DGT (RECEME).

La aplicación realiza desde el negocio las consultas hacia los servicios de la DGT tanto de consulta de puntos como de multas del registro de infractores de la DGT. Además de estas consultas contra la DGT, la aplicación permite consultar las multas del procedimiento Sancionador de la Dirección de Tráfico del Gobierno Vasco. Para ello el sistema se integra con el proyecto A46-Documentación de Sanciones que permite nutrirse de dicha información.

b) adaptación del servicio web de asignación/actualización de los datos de cursos e integración con ANCOREX/RECEME

El actual servicio web permite a aplicación de Gestión Cursos de Sensibilización y Reeducación Vial de las propias Autoescuelas la asignación y actualización de los datos de cursos e integración con ANCOREX/RECEME de la DGT. El servicio implementa las siguientes operaciones para integrarse con la información necesaria a gestionar por la Dirección de Tráfico y la DGT:

- calcular código de curso: proporciona el código utilizado para la identificación de un curso nuevo.
- actualizar datos de curso: integra información referente a un curso ya finalizado gestionado por el nuevo sistema para el posterior envió de anotaciones ANCOREX.
- comprobar incidencias de remesas: proporciona información sobre si el envío de las remesas a la DGT con los datos de los cursos, alumnos y resultado ha sido correcto.
- cumple requisitos medida reeducadora: determinará si el asistente a un curso cumple o no los requisitos para apuntarse al mismo

Será necesario migrar el proceso de negocio actual a Weblogic y adaptar el Business Service de integración ESB Oracle Service Bus 12c con el nuevo proceso de negocio.

c) procesos batch de envío de remesas RECEME y anotación de cursos ANCOREX

Este proceso de negocio, a migrar de WAS a Weblogic, cubre las siguientes funcionalidades por medio de las siguientes operaciones:

- Envío de remesas RECEME
- Procesamiento de las respuestas de remesas RECEME enviadas. Para ello se procesa de los emails existentes en un buzón de correo el XML adjunto, registra en B.D. y se comprueba la firma digital. Según el caso se modifica el estado del mismo.
- Envío de anotaciones ANCOREX
- Procesamiento de las respuestas anotaciones ANCOREX: Se reciben las respuestas de la DGT en forma de XML y se recorre cada anotación y procesando las respuestas según sea el caso.

Se deberán adecuar los distintos JOB's Control-M anteriores y que los scripts invoquen al nuevo negocio.

Los datos de las tablas que gestionan las aplicaciones web se consumen también por aplicaciones HOST por lo que no requiere migración de BBDD.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	DB2
Integraciones	Servicios DGT RECEME/ANCOREX Servicio horizontal de Auditoria de accesos. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA. Servicio Horizontal de Correo: Actualmente la aplicación recupera a partir de un buzón funcional y de manera nativa los mails que la DGT está depositando de los procesamientos de las respuestas de remesas RECEME y anotaciones ANCOREX enviadas. Será necesario hacer uso del servicio Horizontal de Correo. El aplicativo genera diversos documentos en formato PDF mediante Apache FOP. Deberá actualizarse para generarse haciendo uso de JasperReports. 4 procesos Control-M

LOPD	La aplicación debe auditar las peticiones realizadas tanto de las consultas como de la gestión de peticiones contra la DGT realizadas a través del Servicio Horizontal de Auditoria de Accesos

3.2.6.10. A46 – Documentación Sanciones

Descripción funcional

El sistema lo engloba un conjunto de aplicaciones y servicios relacionados con la gestión de información y documentación asociada a los expedientes sancionadores de tráfico.

Entre las aplicaciones web y servicios que ofrece el sistema objeto de la migración se encuentran las siguientes:

a) consulta/Gestión de documentación de sanciones sobre el portal intranet (Gurenet)
b) incorporación masiva de nueva documentación de sanciones desde HOST
c) borrado de expedientes caducados
d) Gestión de certificados

El acceso a las distintas aplicaciones estará restringido por un conjunto de grupos LDAP que tienen acceso a los portlets de Gurenet y que accederán según el caso a los recursos de la aplicación (ACL).

a) consulta/Gestión de documentación de sanciones Gurenet

La aplicación permite acceder a los expedientes sancionadores y visualizar su información básica: datos del expediente, las fechas asociadas al expediente y la información económica.

A su vez se posibilita consultar documentación asociada a los expedientes y adjuntar nueva documentación de manera manual. Cada vez que se adjunte un nuevo documento, las personas que tengan acceso a esta aplicación tendrán la posibilidad de abrir y descargarse los documentos que se hayan adjuntado.

La aplicación ofrece al personal tramitador documentar una guía con los pasos del expediente, que permitirá realizar todo tipo de anotaciones que sean de utilidad para las personas que tengan que trabajar con los expedientes.

La seguridad de la aplicación se gestiona por medio de roles de aplicación (gestores, gestores/borradores y lectores). Estos roles por medio de los ACL's podrán acceder a recursos de aplicación según sea el caso.

A continuación, se muestra un resumen con la relación de las funcionalidades más importantes que ofrece la aplicación de Documentación de Sanciones:

- Realizar búsquedas de expedientes por diferentes criterios.
- Visualizar los datos principales de un expediente incluyendo denuncia, infractor, fechas asociadas y datos económicos.
- Adjuntar nuevos documentos a un expediente.
- Realizar búsquedas de documentos por diferentes criterios.
- Visualizar los datos de detalle de un documento.
- Abrir un documento y descargar un documento.
- Añadir pasos a la guía de un expediente.
- Imprimir la guía de un expediente.
- Abrir todos los documentos de un expediente en un único fichero PDF.
- Notificar un expediente a una o varias personas de la Dirección de Tráfico.

b) incorporación masiva de nueva documentación de sanciones desde HOST

Además de las aplicaciones web disponibles, el sistema posibilita a la aplicación del Procedimiento Sancionador HOST desde su negocio incorporar nueva documentación a los expedientes de forma masiva. Para ello se implementan una serie de flujos IBM ACE para la recepción de nuevas peticiones de documentación que se canalizarán a los procesos de negocio para su ejecución.

La arquitectura utilizada para realizar la consulta/gestión masiva de expedientes y documentación de los puntos a), b) engloba una serie de componentes distribuidos sobre

los servidores WPS, WAS, Buses de integración ESB Oracle Service Bus 12c/IBM ACE y que serán necesarios migrar a la nueva arquitectura:

- migración de la aplicación web a Liferay
- migración del flujo integración IBM ACE para la consulta de los atributos HOST a ESB Oracle Service Bus 12c
- migración del flujo integración IBM ACE para la consulta de un expediente sancionador ESB Oracle Service Bus 12c
- migración del flujo integración IBM ACE gestión de los nuevos expedientes originados desde HOST a procesar en el sistema a ESB Oracle Service Bus 12c
- migración del actual proceso Listener (MDB) de carga masiva de documentos a ESB Oracle Service Bus 12c

Las funcionalidades descritas a) y b) hacen uso de los servicios horizontales para proveer de la información necesaria:

- servicio del gestor Documental
- antecedentes ATEX de la DGT

c) Borrado de expedientes caducados

Proceso batch que se encarga de eliminar aquellos registros de expedientes de BBDD que han sido consultados tanto desde la consulta de documentación de Sanciones y la generación de la carta de pago y cuya fecha límite de la infracción es menor a la fecha actual.

Actualmente existe un JOB Control-M encargado de ejecutar este proceso.

d) Gestión de certificados

La aplicación permite la gestión de los dispositivos y los certificados de la vía relacionados a las sanciones impuestas por la Dirección de Tráfico en su procedimiento sancionador, pudiéndose dar de alta, modificar y anexar los certificados.

La aplicación se integra con el gestor documental corporativo para el anexo de certificados.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	DB2 HOST
Integraciones	Flujo de integración IBM ACE para la consulta de los atributos HOST asociado a cada documento de sanción. Flujo de integración IBM ACE para la consulta de un expediente sancionador Flujo de integración IBM ACE para la gestión de los nuevos expedientes originados desde HOST a procesar en el sistema. Integración con el Servicio Horizontal "Kudok" de Gestión Documental Antecedentes ATEX de la DGT El aplicativo genera diversos documentos en formato PDF mediante Apache FOP. Deberá actualizarse para generarse haciendo uso de JasperReports. Auditoría de accesos. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA. 1 proceso Control-M
LOPD	La aplicación deberá auditar las peticiones realizadas tanto de las consultas como de la gestión de documentación de sanciones realizadas, a través del Servicio Horizontal de auditoría

3.2.6.11. A47 – Registro de Policías locales

Descripción funcional

El presente aplicativo tiene como objetivo principal la gestión del registro de policías locales de la Comunidad Autónoma de Euskadi.

Está compuesto por seis aplicaciones web, construidas como portlet, que dan la funcionalidad completa al aplicativo.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales desde la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para los usuarios del Departamento de Seguridad añadiendo los perfiles de usuario que sean necesarios. Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto y consumido por la aplicación en proceso de migración mantenga su funcionamiento.

En general, dentro del registro, las personas usuarias con un rol asignado a la policía local, solamente tienen acceso a la información que corresponde a su centro, mientras que las personas usuarias asignadas a un rol del Departamento (nuevo a crear), tienen acceso al registro completo.

El listado de aplicaciones web son las siguientes, la última debe migrarse también la parte de presentación de forma completa. El resto deberá adecuarse la presentación para la incorporación del nuevo rol a crear:

- **Registro de ayuntamientos**: esta aplicación permite el alta, consulta, búsqueda y gestión de los datos de los ayuntamientos de la CAE que cuentan con policía local, permite la gestión de los municipios, mancomunidades, sedes y direcciones, personas de contacto, RPT, así como de distinta documentación: actos, acuerdos, convenios, etc.

- **Registro de Policías Locales**: esta aplicación permite el alta, consulta, búsqueda y gestión de los datos de una Policía Local tales como los turnos de servicio, los protocolos y convenios que mantienen con la Dirección de la Ertzaintza, las funciones y dotaciones, los medios y equipamientos, así como la relación de armas que mantiene en la actualidad o ha gestionado en el pasado.
- **Registro de agentes**: esta aplicación permite el alta, consulta, búsqueda y gestión de los datos de los agentes de las distintas policías locales de la CAE. Dentro de la aplicación se permite mantener los datos personales del agente, la plaza que ocupa, la formación, tanto profesional como académica, las menciones o sanciones recibidas y la relación de armas que tiene o ha tenido asignada un agente.
- **Registro de armas:** esta aplicación permite el alta, consulta, búsqueda y gestión de los datos de las distintas armas que pertenecen o han pertenecido a las distintas policías locales de la CAE. La aplicación mantiene un catálogo con los datos identificativos de las armas, las revistas realizadas sobre ellas, así como las incidencias que se han producido en su uso.
- **Informes**: la aplicación de informes permite obtener estadísticas e informes en formato PDF y Excel a partir de los datos del registro, tales como estadísticas de los agentes o el informe de las revistas de las armas.
- **Tabla de códigos**: esta aplicación permite la gestión de los datos de tablas de códigos de los que hacen uso el resto de aplicaciones que forman el registro de policías locales.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Portlet 1.0, Struts Framework Portlet Java 1.8, Portlet 2.0, JSF2.2, Primefaces 8.0 (Liferay)
Persistencia	Oracle 19c
Integraciones	Integración con el Servicio Horizontal “Kudok” de Gestión Documental

	El aplicativo actual envía correos haciendo uso de la librería Oinarri, deberá hacer uso del servicio horizontal de envío de correo B71. El aplicativo actual utiliza la librería Oinarri para registro de auditoría LOPD, deberá integrarse con el Servicio Horizontal Registro Auditoría. La aplicación actual se integra con DB2 Host para consultar tablas maestras de datos. Un proceso Control-M
Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP. Funcionalmente se definen tres perfiles: los usuarios con permiso de edición (jefe de policía, inspección y administrativo, que tendrán acceso a los datos de su centro); el personal del ACPL que tendrá acceso a los datos de todos los centros (en algunos casos solo en modo consulta y en otros de edición); y los usuarios con permiso de lectura, que serán los agentes de policía local.
LOPD	Todas las acciones de alta/modificación/baja/consulta sobre el registro de policías locales deberán ser registradas mediante el Servicio Horizontal de Auditoría

3.2.6.12. A91 – Viabilidad Invernal

Descripción funcional

Vialidad Invernal es una aplicación que permite gestionar el estado en el que se encuentran los principales puertos y tramos tanto de la CAPV como de fuera de ella.

Esta aplicación permite conocer en todo momento cuál es el estado de los puertos y tramos gestionados, actualizar su estado, y ver toda esta información sobre un mapa de carreteras en el que se mostrarán únicamente aquellos puertos y tramos que tengan algún problema circulatorio debido a su estado. Además de esto, también permite la posibilidad de incluir en la aplicación nuevos tramos y puertos de montaña a gestionar.

Hoy en día, existe una aplicación en la web de Tráfico (www.trafikoa.euskadi.eus) que ofrece información de Vialidad Invernal a partir de la información registrada en esta aplicación.

La aplicación consta de dos secciones principales:

- Estado de Puertos y tramos: En esta sección se gestionan las restricciones de acceso y circulación para los distintos tipos de vehículos (turismo, camión, articulados). Permite la búsqueda filtrada de puertos y tramos y se muestran su estado y geolocalización dentro de un visor cartográfico.
- Administración de puertos y tramos: Esta sección es la encargada del alta, baja y modificación de cada uno de los puertos y tramos de carretera susceptibles de ser gestionadas desde la aplicación.

Toda modificación realizada sobre los puertos y tramos pasa por un estado de “staging” en el cual los usuarios de la aplicación pueden visualizar las modificaciones realizadas, con objeto de que sean validadas, antes de ser publicadas en el portal de Trafikoa.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1, SpringJDBC
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	DB2 LUW
Integraciones	Servicio Horizontal Callejero NORA. Actualmente la aplicación no hace uso del servicio de horizontal de callejero Nora para mostrar la información de provincias. El nuevo aplicativo deberá integrarse con este servicio. API visor mapas Arcgis: Se deberá actualizar para hacer uso del API GIS Motorea. Servicio Horizontal de Correo. Actualmente la aplicación envía los correos mediante SMTP. La nueva aplicación deberá integrarse con el Servicio Horizontal de Correo .
Seguridad	Sólo existe un perfil con acceso a esta aplicación
LOPD	No se requiere

3.2.6.13. A91 – Cámaras de Tráfico

Descripción funcional

La aplicación de Cámaras de Tráfico es una aplicación de trabajo que permite gestionar toda la información acerca de la ubicación de las cámaras de la Comunidad Autónoma del País Vasco.

Desde esta aplicación se puede saber dónde están situadas todas las cámaras de la CAPV, conocer su ubicación física sobre un mapa de carreteras y añadir nuevas cámaras que sean instaladas por la Dirección de Tráfico.

Hoy en día, existe una aplicación en la web de Tráfico (www.trafikoa.euskadi.eus) que ofrece información de las cámaras y está integrada con esta aplicación.

A continuación, se muestran todas aquellas operaciones que la aplicación permite realizar:

- Búsquedas:
  - Búsqueda de cámaras por distintos criterios.
  - Modificación de los datos de la cámara
- Cámara:
  - Dar de alta una cámara.
  - Suprimir la visualización de una cámara.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	DB2 LUW

Integraciones	Integración con Servicio Horizontal NORA. Actualmente la aplicación no hace uso del servicio de horizontal de callejero Nora para mostrar la información de provincias, carreteras, municipios…etc. La nueva aplicación deberá hacer uso del Servicio Horizontal destinado a tal efecto.
Seguridad	Sólo existe un perfil con acceso a esta aplicación
LOPD	No se requiere

3.2.6.14. B52 – Gestión de Radares

Descripción funcional

Radares es una aplicación de trabajo que permite gestionar toda la información acerca de la ubicación de los radares fijos de la CAPV.

Esta aplicación permite conocer dónde están situados todos los radares fijos de la CAPV, ver su ubicación física sobre un mapa de carreteras, así como añadir nuevos radares que sean instalados por la Dirección de Tráfico.

Hoy en día, existe una aplicación en la web de Tráfico (www.trafikoa.euskadi.eus) que ofrece información de los radares a partir de la información registrada en esta aplicación.

La aplicación consta de una única sección en la que se pueden realizar las siguientes acciones:

- Búsqueda de radares: Filtro de búsqueda por los distintos atributos de un radar y listado de resultados
- Visualización cartográfica de radares: Visor cartográfico en los que se muestran los distintos puntos correspondientes con los radares gestionados por la aplicación.
- Consulta/Alta/Baja/Modificación de ficha de radar: Vista en detalle de los atributos de un radar en el que se permite el alta/baja/modificación de un radar.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, Java EE 6, EJB 3.1
Tecnologías de presentación	Java 1.7, Struts Framework Portlet, IBM Portlet
Persistencia	DB2 LUW
Integraciones	API visor mapas Arcgis. Se deberá actualizar para hacer uso del API GIS Motorea.
Seguridad	El acceso a la aplicación estará restringido.
LOPD	No se requiere
Mejoras	Actualmente en la sección de Gurenet "Soporte y Utilidades" existe un portlet en el que se muestra lo mismo que en el portal de Trafikoa. Este portlet de visualización no es necesario migrarlo y en su lugar se sustituirá por un enlace a la página análoga del portal de Trafikoa.

3.2.6.15. B89 – RVATE

Descripción funcional

RVATE es el Registro de Víctimas de Accidentes de Tráfico de Euskadi. Esta aplicación permite a las policías locales registrar las víctimas de accidentes de tráfico, así como consultar en detalle los accidentes registrados de su municipio. A su vez, posibilita a la Dirección de Coordinación de Seguridad tener un registro único y global con los accidentes de las diferentes policías locales para su consulta y registro y adicionalmente ofrece a la Dirección de Tráfico tener un registro de consulta con los accidentes gestionados por la Ertzaintza.

Se podrán consultar todos los detalles del accidente como características (calzada, velocidad, número de carriles, sentido, zona, …), circunstancias (estado meteorológico, iluminación, superficie, …), secuencia, vehículos implicados o personas implicadas.

Funcionalmente las personas con acceso a la extranet del Departamento, accesible para las policías locales, pueden realizar consultas y gestionar accidentes de su municipio y consultar vehículos y personas. Desde el portal de la intranet existen 2 roles (Dirección/Encargados de Coordinación de Seguridad y Dirección de Tráfico) que pueden consultar/gestionar accidentes de las policías locales y/o consultar accidentes de la Ertzaintza según el rol que tengan.

La parte de presentación de esta aplicación está en proceso de migración a Liferay y es accesible para las policías locales en la extranet del Departamento. Deberá adaptarse la capa de presentación para que sea también accesible para las personas del Departamento de Seguridad añadiendo los perfiles anteriormente citados. Además de migrar la seguridad de la aplicación, la actual aplicación de la intranet cuenta con una serie de funcionalidades que deberán incorporarse a la versión Liferay en proceso de migración.

Así mismo, se deben migrar los desarrollos de la capa de negocio al nuevo entorno tecnológico, manteniendo o adaptando el API expuesto.

Tecnologías e integraciones

Tecnologías negocio	Java EE7, EJB 3.1
Tecnologías de presentación	Java EE7, Portlet 2.0, JSF 2.0 (Liferay)
Persistencia	JPA 2.0
Integraciones	Integración con el Servicio Horizontal de gestión documental Kudok Integración con el Servicio Horizontal Registro Auditoría. El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA.

Seguridad	Acceso controlado en presentación mediante pertenencia a grupos de LDAP: director/encargado de DCPL y Dirección de Trafico con 2 perfiles de seguridad diferenciados
LOPD	Todas las acciones realizadas se deberán seguir registrando registrar en el módulo de auditoría.

3.2.6.16. B61 – Embajadas y consulados

Descripción funcional

La aplicación de Embajadas y consulados tiene como objetivo poder registrar los datos de embajadas, consulados y otros organismos. Una vez registrados estos datos, podrán ser consultados por los y las usuarias autorizadas.

Por lo tanto, las personas usuarias de la herramienta están englobados en 2 perfiles diferenciados. Por una parte, existe el perfil administrador y por otro lado el de visualizador de datos públicos.

El rol administrador podrá:

- Dar de alta, modificar y eliminar todo tipo de organismos y sus datos asociados. Esto es, dar de alta nuevas embajadas, consulados y otros organismos, modificar sus datos y borrarlos. Una vez seleccionada la entidad con la que se desea trabajar (embajada o consulado), se accederá a una pantalla de selección para poder filtrar los registros deseados.
- Los datos de las embajadas estarán divididos en datos comunes (Nombre, Sede, Dirección, Datos contacto, etc..) y datos sensibles (Personas de contacto y medios, fiesta nacional, visitas, Estrategia a aplicar, Incidencias). El mantenimiento de estos datos se realizará a través de una consulta donde se podrán seleccionar los registros que se deseen para poder realizar su mantenimiento.

- Crear varios contactos para cada tipo de organismo.
- Se podrán gestionar los contactos de la embajada con sus datos comunes (como el Nombre, Cargo, Teléfono, fax, email público) y sus datos sensibles (Fotografía, Tipo de relación, Fechas, Hechos significativos, tarjeta de visita, etc…)
- Exportar a una hoja excel todos los datos consultados de embajadas, consulados, otros organismos y sus contactos principales. Se visualizará en forma de aviso un mensaje del día de fiesta nacional más cercana de una embajada o de un consulado.

Usuarios/as consultores de datos tanto de embajadas como de consulados pueden ver los datos comunes, pero no pueden ver los datos sensibles.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1, SpringJDBC
Tecnologías de presentación	Java 1.7, IBM Portlet, Struts Framework Portlet
Persistencia	Oracle 19c
Integraciones	Servicio Horizontal Callejero NORA Integración con el Servicio Horizontal “Kudok” de Gestión Documental El nuevo aplicativo deberá integrarse con el Servicio Horizontal de auditoría publicado por la librería GIDA.
Seguridad	El acceso a la aplicación estará restringido. Existen 2 perfiles en la aplicación de Embajadas y consulados: administrador y visualizador de datos públicos.

LOPD	Se requiere integración con el Servicio Horizontal de Auditoría

3.2.6.17. B67 – Dudatan

Descripción funcional

La aplicación Dudatan tiene como objetivo facilitar a las personas la posibilidad de realizar consultas relacionadas con el uso del euskera. Así mismo, ofrece las funcionalidades necesarias para que desde el Área de Normalización puedan gestionarse las mismas.

Las personas con permisos a realizar consultas podrán:

- Realizar una consulta: es decir, puede registrar una pregunta rellenando un formulario con sus datos y la pregunta. El servicio de normalización lingüística recibe un mail indicando que se ha registrado una pregunta
- Cada cual podrá consultar sus consultas realizadas y ver la respuesta facilitada por las y los gestores. Si está rechazada, tendrá acceso al detalle del rechazo. Además, podrá responder al técnico si la consulta está en estado de finalizada o rechazada. Los posibles estados son: pendiente, en curso, finalizada, rechazada.
- Visualizar el listado de consultas públicas: es decir, se podrán visualizar aquellas preguntas y respuestas realizadas por otras personas y que desde el Área de Normalización se hayan categorizado como públicas.
- Contestar una encuesta de satisfacción.

Las personas gestoras que responde las consultas disponen de las siguientes funcionalidades:

- Consultar las consultas realizadas: esto es, visualizará las consultas realizadas y dispondrá de filtros de búsqueda.

- Tramitar las consultas: podrá acceder al detalle de cada consulta para tramitarla, responderla, rechazarla o finalizarla. Podrá guardar un borrador de su respuesta. La respuesta del técnico se guardará junto con que realizó la respuesta, la fecha en que la realizó y un cuadro de texto no editable con la respuesta. La tramitación de la respuesta cambiará de estado y enviará un email a la persona que realizó la consulta con la respuesta facilitada.
- Consultar las consultas públicas: se podrán ver las consultas que se han categorizado como públicas y ver la bitácora de dicha consulta.
- Consultar las estadísticas de las consultas: se podrá visualizar:
  - El número de consultas en las que la respuesta se ha recibido a tiempo.
  - El número de consultas en las que la respuesta no se ha recibido a tiempo.
  - El número de consultas en las que la respuesta ha sido válida para la persona usuaria.
  - El número de consultas en las que la respuesta no ha sido válida para la persona usuaria.

Tecnologías e Integraciones

Tecnologías negocio	Java 1.7, J2EE 1.4, EJB 2.1
Tecnologías de presentación	Java 1.7, IBM Portlet, Struts Framework Portlet Se utiliza el componente de calendario
Persistencia	Oracle 19c
Integraciones	Servicio Horizontal de Correo
Seguridad	El acceso a la aplicación estará restringido. Usuarios/as de la herramienta están englobados en 2 perfiles diferenciados:

	• PERFIL_PREGUNTA: personas que introducen las consultas • PERFIL_RESPONDE: quienes gestionan las mismas
LOPD	No se requiere de integración con el Servicio Horizontal de Auditoría

3.3. Consideraciones generales

Las siguientes consideraciones generales hacen referencia a ambos lotes.

Los proyectos que se plantean migrar en este documento son proyectos vivos a los que se aplican con cierta frecuencia desarrollos evolutivos, correctivos y/o perfectivos. Correrá por cuenta del adjudicatario, sin coste adicional, trasladar estos cambios a la aplicación que se está migrando.

El Departamento de Seguridad está inmerso en un proyecto de migración del actual sistema Host, denominado zBerritu, el cual puede afectar a las aplicaciones objeto del pliego.

3.3.1 Calidad y seguridad del código entregado

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

a) Herramientas de análisis estático de código

b) Auditorías en las que se podrá realizar una inspección y revisión manual del código.

3.3.2 Cobertura en pruebas automatizadas

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

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

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

3.3.3 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 umbral definido cada aplicación se comunicará al inicio del proyecto ya que la Dirección cuenta con informes estadísticos DataWarehouse que permiten conocer los tiempos de respuesta actuales.

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

3.3.4 LOPD

La mayoría de las aplicaciones realizan acciones que por la LOPD exigen una auditoría completa y detallada de las acciones que se realizan. Es requisito indispensable que los nuevos aplicativos mantengan la auditoría de acciones adaptada a la nueva librería “GIDA”, que mantiene un alto grado de compatibilidad a nivel de API con los sistemas previos.

Existen aplicaciones actuales que carecen de esta auditoría o la misma no es completa; el proyecto de migración deberá incluir la revisión de la misma como mejora.

3.3.5 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.

3.3.6 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 del lote 1 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. EJECUCIÓN DEL CONTRATO

4.1. Planificación y organización

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

La correcta planificación y organización van a ser las estrategias que permitirán distribuir el tiempo disponible de la forma más racional posible, permitiendo la priorización de tareas.

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 portales y 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 unas librerías de desarrollo propio y cuya presentación se implementa sobre los portales objeto de este pliego.

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

Nota.

Es posible que tanto a lo largo de la vida del contrato como en sus etapas previas puedan cambiar tanto las versiones como los productos que se citan.

Capa de seguridad

- MicroSoft Forefront TMG
- Oracle HTTP Server 12c (12.2.1.4)
- Oracle Access Manager 12c (12.2.1.4)
- Active Directory 2019
- Oracle Unified Directory 12c (12.2.1.4)

Gestión de portales y servidor de aplicaciones

- JBoss 7.4 y Liferay DXP 7.3
- Oracle WebLogic Server 12c (12.2.1.4)

Desarrollo de Portlets

- Portlet 3.0 (JSR 286), Java Server Faces 2.2, PrimeFaces 11

Desarrollo de EJBs

- EJB 3.2 + JPA 2.1

Middleware de intercambio de información

- Oracle Service Bus 12c (12.2.1.4)
- Mensajería IBM MQ 9.2

Automatización de procesos

- Control-M
- Apache Ant
- Gradle

Gestión documental

- IBM Content Manager v8.5

Frameworks y estándares

- Todos los desarrollos deben realizarse para la versión 8 de la JDK
- Framework internos: GIDA

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

Servidor de bases de datos

- Oracle RAC 19c
- SQL Server 2019
- DB2 z/OS 12.1
- DB2 LUW 11.5

Plataforma GIS

- ArcGIS Portal 10.7.1

Repositorio de código fuente

- Azure DevOps Server 2020

Repositorio documental de proyecto

- Microsoft SharePoint 2016

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

- Se encargará de la gestión operativa del proyecto, coordinando al equipo de desarrollo.
- Se encargará de la gestión del plan y del aseguramiento de la calidad del Proyecto
- Se responsabilizará del seguimiento de las especificaciones técnicas realizadas por el analista.

- Colaboración con el equipo de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, para orientar las soluciones óptimas a las necesidades que dicho equipo plantee a nivel de infraestructura y plataforma base.

Arquitecto técnico

- 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.
- Se responsabilizará de colaborar con el equipo de Oficina Técnica de Gestión del Software (OTGS) de la DGTSI para el traslado de propuestas y solicitar la validación de soluciones sobre la arquitectura y el desarrollo del proyecto.

Analista / Desarrollador

- Elaboración de las especificaciones técnicas de la solución, así como preparación de su despliegue en los entornos del Departamento de Seguridad
- Realizarán desarrollo y pruebas sobre las funcionalidades específicas.
- Preparación técnica y documental de los paquetes de versión necesarios para la implantación de las versiones necesarias.

4.4. Gestión de la calidad

La DGTSI establece los procedimientos de calidad definiendo aquellas pautas necesarias que logren un aseguramiento de la calidad de procesos, productos y servicios, y evalúe de forma objetiva las actividades software enmarcadas en el presente contrato.

Con objeto de mejorar progresivamente la calidad del software incluida en el ámbito del presente pliego de bases técnicas, el adjudicatario deberá realizar las tareas definidas en el Plan de Calidad del Departamento de Seguridad. Entre los aspectos a contemplar estarán los siguientes:

- controles de calidad para los entregables (documentación) que se hayan visto afectados;

- pruebas unitarias que eviten la introducción de un nuevo defecto al intentar reparar el error que se pretendía corregir;
- pruebas de integración ejecutadas para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos;
- pruebas de sistema que 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; y
- realización de los test de calidad, así como solicitud de la auditoría de calidad al equipo de la DGTSI encargado de dicha tarea.

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

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

No se permitirá la puesta en producción a aquellas aplicaciones que no cumplan unos mínimos en cuanto a rendimiento, calidad y protección ante vulnerabilidades.

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

Los productos entregables que se revisarán durante los procesos de auditoría de Calidad son de código fuente y documental tanto de proyecto como de producto. Para cada una de las fases existen herramientas y plantillas tipo que facilitará cumplimentar la información para cada entregable requerido.

- Fase gestión
    - Planificación y seguimiento del proyecto haciendo uso de las herramientas y plantillas de gestión definidas por normativa.
- Fase funcional
    - Documento de requisitos con la identificación de los requisitos funcionales/no funcionales del Sistema.
    - Análisis funcional con la descripción funcional del sistema e identificación de los procesos.
    - Casos de Uso con la definición de las secuencias de interacciones (pasos/actividades) que deberán realizarse para llevar a cabo entre los procesos del sistema y sus actores.
- Fase técnica
    - Arquitectura del sistema con el diseño a de la arquitectura y descripción de los componentes de la arquitectura junto sus relaciones.
    - Diseño físico de datos con el esquema físico de la base de datos y descripción de los objetos utilizados.
    - Volumetría del volumen estimado de las tablas e índices de BBDD.
    - Interface de usuario/a con el diseño de los interfaces de usuario/a 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 uso según perfil.
  - Manual de explotación que recogerá el conjunto de tareas que se deberán realizar para la correcta explotación del sistema.

Todos los elementos producto del desarrollo y ejecución del contrato deberán quedar albergados en los servidores corporativos del Departamento de Seguridad, con la estructura que se habilitará al efecto y cumpliendo con las normativas internas definidas salvo que se indique expresamente lo contrario. Esto incluye código fuente, archivos binarios, ejecutables, contenidos estáticos, scripts de cualquier tipo (creación o adaptación de base de datos, construcción y empaquetado del producto, etc.), ficheros de configuración, certificados, etc., así como toda la documentación asociada: planificación, requisitos, análisis, diseño, pruebas, implantación; manuales de uso, mantenimiento, configuración, construcción y empaquetado; actas de reunión, informes de avance, etc. En cualquier momento del desarrollo y ejecución del contrato se podrá solicitar a la empresa adjudicataria la entrega de cualquier o todos estos elementos para su validación y control.

4.5. Normas de seguridad relativas a los sistemas de información

La empresa adjudicataria se compromete a cumplir las normas respecto a los sistemas de información del DSGV recogidas en el Anexo 1. Normas de seguridad relativas a los sistemas de información.

4.6. Registros, notificaciones e Inventarios

Como parte del contrato, la empresa adjudicataria estará obligada a dar total cumplimiento a las condiciones que al efecto de control establezcan el técnico o técnica del Gobierno Vasco.

La empresa adjudicataria deberá proporcionar la información requerida por el Gobierno Vasco para conocer la situación y desarrollo de los servicios contratados. Esta información se proporcionará en forma de informes que deberán presentarse de forma periódica.

La elaboración de estos informes periódicos tiene carácter obligatorio y será entregado al técnico o técnica responsable del Gobierno Vasco junto con la facturación.

4.7. Lugar de ejecución del contrato

La prestación del servicio se realizará en la empresa adjudicataria, pero con presencias puntuales en las oficinas de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, Erandio, por requisitos del proyecto en la realización de tareas concretas que así lo requieran.

5. DOCUMENTOS ANEXOS

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

La empresa adjudicataria se compromete a cumplir las siguientes normas de comportamiento respecto a los sistemas de información del DSGV:

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

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

- Los equipos conectados a la red corporativa del DSGV no podrán conectarse a ningún sistema informático o de telecomunicaciones ajeno al Departamento
- Los equipos o sistemas que por su actividad requieran conexión a servicios externos al Departamento deberán estar aislados, es decir, separados física y lógicamente de la red informática del DSGV
- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del Departamento de Seguridad

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.

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/la usuario/a (red doméstica) o su empresa.
- Los equipos contarán con un lector de tarjetas digitales para la autenticación de usuario/a.
- 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 usuarios/as

Usuarios/as autorizados/as 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/la usuaria 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/a sin permisos de Administrador Local.
- El/la usuaria 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.

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.