



SEGURTASUN SAILA

Adminiseta Zerbitzuen Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak
Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD

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

**EVOLUCIÓN EUSKARRI -
MIGRACION HIBERNATE A JPA**

PLIEGO DE PRESCRIPCIONES TÉCNICAS



TABLA DE CONTENIDOS

	Página
1. ANTECEDENTES Y OBJETO DEL PLIEGO	2
2. ALCANCE DEL CONTRATO.	3
3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS.....	4
3.1. FUNCIONALIDADES EUSKARRI	5
4. ENTREGABLES	8
5. EJECUCIÓN DEL CONTRATO	9
5.1. PLANIFICACIÓN Y ORGANIZACIÓN.....	9
5.2. ENTORNO TECNOLÓGICO.....	9
5.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO	11
5.4. GESTIÓN DE LA CALIDAD	12
5.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN	14
5.6. REGISTROS, NOTIFICACIONES E INVENTARIOS.	15
5.7. LUGAR DE EJECUCIÓN DEL CONTRATO.	15
DOCUMENTOS ANEXOS.....	16
ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN.....	16



1. ANTECEDENTES Y OBJETO DEL PLIEGO

El Decreto 6/2021, de 19 de enero, por el que se establece la estructura orgánica y funcional del Departamento de Seguridad, en su artículo 13, establece que corresponde a la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, en adelante DGTSI, lo referente a la planificación, gestión y mantenimiento de los sistemas destinados a actividades de seguridad pública. A tal fin le corresponde, entre otras actividades, la provisión y mantenimiento de sistemas de información y comunicaciones necesarios para el cumplimiento de las funciones que incumben al sistema vasco de seguridad pública, así como la de prestar servicios informáticos y de comunicaciones al Departamento de Seguridad del Gobierno Vasco.

Euskarri es el aplicativo utilizado actualmente por la Dirección de Atención de Emergencias y Meteorología (DAEM) para la gestión de incidencias y su coordinación con las diferentes agencias con las que colabora: Ertzaintza, Osakidetza Emergentziak, Centro de Gestión de Tráfico de Euskadi y Servicios de Bomberos de las Diputaciones Forales y de los diferentes Ayuntamientos.

Este sistema se implementó en el año 2010 y se le han ido incorporando entidades de forma progresiva hasta el año 2021. Aunque en su día se utilizó la tecnología más adecuada del momento, actualmente su arquitectura está obsoleta siendo necesaria su renovación y adecuación a las alternativas actuales.

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 las condiciones de ejecución a las que debe ajustarse el servicio solicitado.



2. ALCANCE DEL CONTRATO.

Desde el inicio de la aplicación, para acceder a los datos que se almacenan en la base de datos Oracle, se utiliza la herramienta Hibernate como sistema de ORM (mapeo objeto-relacional). La versión utilizada es obsoleta y, por ello, es necesario su actualización. Dado que el estándar utilizado en la DGTSI para la persistencia y la correlación relacional de objetos y funciones para las especificaciones relativas a EJB 3.X es JPA (Java Persistence API), ésta deberá ser la solución a desarrollar para la actualización del aplicativo Euskarri.

Adicionalmente, y con el objeto de optimizar el rendimiento del aplicativo Euskarri, será necesario evolucionar los elementos de negocio de la versión actual EJB 3.0 a EJB 3.2.

La solución a implementar se deberá modernizar y adaptar a los nuevos estándares de desarrollo y calidad definidos por la DGTSI.

El presente expediente tiene por objeto la contratación de las tareas necesarias de análisis, diseño, desarrollo e implementación para realizar la renovación de la tecnología actual del sistema mediante la implementación de JPA 2.1 integrado con EJB 3.2.

3. DESCRIPCIÓN DE LOS SERVICIOS SOLICITADOS.

Actualmente el modelo de datos de Euskarri utiliza más de 600 objetos entre tablas y vistas. Todos estos objetos deben tener su mapeo correspondiente en JPA para poder trabajar con ellos desde la capa de negocio.

Para llevar a cabo esta renovación tecnológica es necesario adecuar las funcionalidades existentes con el fin de modernizar y mejorar el rendimiento actual del aplicativo.

Entre las tareas a desarrollar cabe destacar las que se enumeran a continuación:

- Creación de repositorios JPA: Los nuevos repositorios deben sustituir a los objetos de negocio actualmente existentes. Los repositorios deberán optimizar (minimizar) los accesos a la base de datos, de forma que no devuelvan más información que la necesaria. Cualquier solución implementada debe funcionar en un sistema distribuido de alta disponibilidad.
- Exponer únicamente aquellos métodos de negocio a los que se pueda invocar desde el cliente como servicios web REST.
- Modificar el actual cliente de Euskarri para que realice la autenticación con el sistema de seguridad, gestione la renovación del token de usuario y se comuniquen con el servidor invocando al nuevo API de servicios web REST securizados expuesto.
- Adaptación de todos los EJB's de negocio a la nueva versión indicada, e integrados con el estándar JPA.
- Revisión y realización de la documentación con el fin de dejar recogida la nueva implementación, así como el inventario de los nuevos elementos creados.

Todos los desarrollos deberán realizarse según la normativa actual establecida por DGTSI, a destacar:

- Sistema de trazas y auditoria que permita conocer la trazabilidad de cada petición originada en el cliente.

- Nomenclatura de métodos y clases, de forma que se permita identificar inequívocamente todos y cada uno de los métodos del negocio.
- Securitización de los servicios REST.

Además, con el fin de minimizar el tráfico en la red departamental, será necesario:

- Optimizar los métodos de negocio para comunicar únicamente la información estrictamente necesaria
- Optimizar el sistema de notificación de Euskarri de forma que se generen sólo las notificaciones necesarias.

3.1. Funcionalidades Euskarri

Sin pretender ser una lista exhaustiva, se citan a continuación las partes funcionales actualmente más importantes del sistema, a considerar en la renovación tecnológica:

- Sistema de Seguridad
 - Roles/Perfiles de usuarios
 - Personal operativo
 - Grabación de rastros de auditoría
- Carta de llamada
 - Transferencias de Cartas de llamada
 - Llamadas especiales (TEPA, PDEA, CENTROS “BEREZI”, BIZI, BORTXA,...)
 - Misión
- Tratamiento de incidentes
 - Gestión datos estructura incidentes
 - Tramitación de los incidentes
 - Incidentes planificados
 - Consultas de incidentes
 - Estados del incidente
 - Cierres de incidentes
- Tratamiento de recursos
 - Definición de recursos

- Gestión de recursos (estados)
- Integración con radio digital
- Plan de acción
 - Propuesta automática
 - Seguimiento
 - Acciones automáticas o diferidas
 - Información de recursos y servicios operativos
 - Cartas de llamada salientes
- Monitores automáticos
 - Monitor de incidentes
 - Monitor de recursos
 - Monitor de llamadas
 - Lista de servicios
- Gestor de conocimientos
 - Textos
 - Filtros
 - Localizadores
 - Integración con tratamiento de incidentes
 - Interface con telefonía
- Sistema topográfico
 - Objetos topográficos (calles, carreteras, ...)
 - Bloques, áreas de operador, sectores
 - Integración con Cartografía (GIS)
- Afectados, vehículos y bienes
 - Afectados (personas evacuadas)
 - Vehículos retirados
 - Bienes afectados
- Herramientas de análisis
 - Consultas
 - Estadísticas e Informes

- Seguimiento Sanitario
 - Diagnósticos médicos
 - Informe asistencial
 - Integración con tratamiento de incidentes
 - Integración con historial del paciente
 - Gestión de Flotas

Todos estos bloques de funcionalidad están soportados en múltiples tablas de datos maestros. Actualmente el aplicativo maneja alrededor de 240 tablas maestras y 130 tablas para cada uno de los tres esquemas relacionados con la parte incidental.

Debido a que Euskarri es una aplicación en continua evolución, el adjudicatario deberá incorporar, sin coste adicional, en sus desarrollos todas aquellas nuevas funcionalidades o modificaciones que pudieran producirse en el sistema actual durante la ejecución del expediente.

Debido al volumen del trabajo a realizar, se han definido seis entregas, que permiten fraccionar las tareas a realizar. Esta agrupación se ha realizado teniendo en cuenta el grado de complejidad de las funcionalidades implicadas en el desarrollo, de forma que se vayan acometiendo de las más sencillas a las más complejas, lo que permita al equipo de trabajo asignado que se adapte progresivamente a la aplicación Euskarri.

Una vez adjudicado el expediente y, durante la incorporación de la empresa al proyecto, la DGTSI entregará al adjudicatario el contenido de cada una de las entregas planificadas.

4. ENTREGABLES

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

Durante la ejecución e implantación del desarrollo del expediente, la empresa adjudicataria deberá cumplimentar todos los documentos definidos como obligatorios dentro de la metodología y ciclo de vida definida por la DGTSI.

Adicionalmente, asociado a cada uno de los hitos definidos en la planificación, el adjudicatario deberá entregar el código generado junto con la plantilla definida por la DGTSI asociada a cada uno de los objetos de la migración.

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

5. EJECUCIÓN DEL CONTRATO

5.1. Planificación y organización

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

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible, permitiéndonos priorizar las tareas más importantes y urgentes.

5.2. Entorno tecnológico

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

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

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

El entorno tecnológico deberá cubrir las tecnologías: Desarrollos Java EE referentes a Euskarri, sin perjuicio de que en un futuro puedan cambiar tanto las versiones como los productos que se mencionan.

Entorno tecnológico ACTUAL:

- Presentación
 - Java FX (GIS)
 - Java Swing

- Negocio
 - EJB 3.2
 - EclipseLink 2.7.11 (JPA2.1)
 - Oracle JDK 1.8
 - JPA 2.1
 - APIs de producto de soporte (coherence, Jasper,...)
- Integración / Middleware de intercambio de información
 - Oracle Service Bus (OSB 12c)
 - JMS
 - IBM MQ 9.2
- Bases de datos
 - Oracle RAC 19c
 - DB2 v12.1(z/OS)
 - DB2 11.5(LUW)
- Capa de Seguridad:
 - Oracle Access Manager 12c
 - Active Directory

Herramientas de desarrollo:

- Desarrollo para aplicaciones y EJBs sobre Oracle Weblogic.
 - Eclipse + plugins Oracle Weblogic Server Tools
 - Servidor local Oracle Weblogic Server 12c (12.2.1.4)
- Desarrollo para aplicaciones y EJBs sobre JBoss.
 - Eclipse + plugins JBoss Tools
 - Servidor local JBoss EAP 7.4
- Desarrollo sobre Oracle Service Bus (OSB 12c)
 - Oracle JDeveloper 12c
 - Servidor local Oracle Weblogic Server 12c (12.2.1.4)
- Repositorio de Datos Azure DevOps Server 2020
 - Microsoft Visual Studio 2010 Team Explorer - Source Control
 - Source Control Team Foundation Version Control (TFVC)
- Base de datos:
 - Oracle SQL Developer

- DBeaver
- Java SE Development Kit
 - Java SE Development Kit (JDK) 8 y posteriores
 - Java SE Runtime Environment (JRE) 8 y posteriores
- Desarrollo Java Swing.
 - Netbeans
- Visualizadores GIS:
 - Esri SDK v.100.4 for java
 - ArcGIS Server 10.9.1
 - ESRI Map Objects 2.3
 - ESRI SDE

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

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

5.3. 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.

5.4. Gestión de la calidad

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

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

- Controles de calidad para los entregables (documentación) que se hayan visto afectados.
- Pruebas unitarias y de integración que permitan la validación de las funcionalidades implementadas.
- Pruebas funcionales de aceptación de usuario (UATs).

- Pruebas de carga o rendimiento, en los casos, que se establezcan en función de la modificación realizada.

El código entregado como resultado del proyecto deberá superar los umbrales de calidad y seguridad establecidos. Estos umbrales están definidos por:

- Herramientas de análisis estático de código; y
- Personal de la DGTSI que podrá realizar una inspección y revisión manual del código.

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

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

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

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

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

- Fase técnica e implantación
 - Documento de diseño técnico
 - Plantillas estandarizadas asociadas a los objetos
 - Plan de Pruebas con la relación de los casos de prueba, descripción de los pasos y resultados esperados
 - Manual de explotación del sistema
 - Otro documento que se vea necesario durante la ejecución del proyecto.

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.

En caso de que se genere algún documento para personas usuarias de la aplicación, éste deberá ser bilingüe (euskera y en castellano) y hacer un uso del lenguaje inclusivo no sexista.

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

5.6. 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.

5.7. 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.

DOCUMENTOS ANEXOS

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

La empresa adjudicataria se compromete a cumplir las siguientes normas de comportamiento respecto a los sistemas de información del Dirección General de Telecomunicaciones y Sistemas Informáticos

- No introducir software informático ajeno al Dirección General de Telecomunicaciones y Sistemas Informáticos
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del Dirección General de Telecomunicaciones y Sistemas Informáticos, 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 Dirección General de Telecomunicaciones y Sistemas Informáticos 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 Dirección General de Telecomunicaciones y Sistemas Informáticos.
- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del Departamento de Seguridad.

1 Acceso y protección de datos

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

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

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

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

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

Esquema Nacional de Seguridad, en lo relativo a lo que establece el RD 311/2022 de 3 de mayo.

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

2 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.