EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA
Administrazio eta Zerbitzuen Sailburuordetza
Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritza

DEPARTAMENTO DE SEGURIDAD
Viceconsejería de Administración y Servicios
Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

GESTIÓN DE INSPECCIONES OCULARES

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Larrauri Mendotxe bidea, 18 – 48950 ERANDIO (Bizkaia)
Tel. 94 607 80 00 – Fax 94 607 83 02

TABLA DE CONTENIDOS

Página

1. ANTECEDENTES Y OBJETO DEL PLIEGO 2

2. ALCANCE DEL CONTRATO 3

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS 5

3.1. ÁREA DE AVISOS 5
3.2. ÁREA INSPECCIONES OCULARES 5
3.3. ÁREA DE ADMINISTRACIÓN 7
3.4. ÁREA DE ANÁLISIS IIOO 10
3.5. INTEGRACIÓN CON APLICACIÓN DE EMERGENCIAS EUSKARRI 10
3.6. INTEGRACIÓN CON EL SISTEMA DE INFORMACIÓN POLICIAL (SIP) 10
3.7. GENERACIÓN DEL INFORME DE INSPECCIÓN OCULAR 11
3.8. CONSIDERACIONES ADICIONALES 11

4. EJECUCIÓN DEL CONTRATO 13

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 13
4.2. ENTORNO TECNOLÓGICO 13
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 15
4.4. GESTIÓN DE LA CALIDAD 16
4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 19
4.6. REGISTROS, NOTIFICACIONES E INVENTARIOS. 20
4.7. LUGAR DE EJECUCIÓN DEL CONTRATO. 20

DOCUMENTOS ANEXOS 21

ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN. 21

1. ANTECEDENTES Y OBJETO DEL PLIEGO

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

Desde la Dirección de la Ertzaintza y, especialmente, desde los Servicios de Investigación Criminal Territoriales surge la necesidad de gestionar de manera eficiente y ágil las investigaciones oculares realizadas en campo por los agentes (creación de una nueva investigación, gestion de evidencias, gestion de almacenes etc.).

Actualmente, los Servicios de Investigación Criminal Territoriales disponen de una aplicación desarrollada mediante ACCESS Forms que cubre parte de las necesidades pero que ha quedado obsoleta debido a las limitaciones que ofrece la tecnología en la que se basa.

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

El objeto de este expediente es la contratación de los servicios para la construcción e implantación del sistema de gestión de inspecciones oculares.

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

2. ALCANCE DEL CONTRATO

El presente expediente tiene por objeto la contratación de las tareas de análisis, diseño, construcción e implantación de la aplicación para la Gestión de Inspecciones Oculares, de cara a poder llevar la gestión relacionada con la recogida, identificación, clasificación y gestión de las evidencias relativas a una inspección ocular realizada en el lugar de los hechos. Todo ello integrado con los actuales sistemas de información policial y de gestión incidental. Dicho desarrollo se presta como una unidad funcional por lo que no procede la división en lotes del contrato.

El nuevo sistema de Gestión de Inspecciones Oculares, tiene además como objetivo fundamental su integración con el Sistema de Información Policial (SIP), alojado en entorno IBM HOST z/OS, donde se realiza la gestión de los atestados elaborados por la Ertzaintza. Así mismo, requiere de integración con el Sistema de Gestión de la Emergencia (Euskarri) que es el encargado de la gestión de las emergencias y alertas del 112. Las funcionalidades a nivel general que debe cubrir la aplicación objeto de este contrato son las siguientes:

a) La gestión de avisos entre unidades: Este módulo es el encargado de gestionar los avisos generados en la aplicación. Otorga la capacidad de emitir mensajes de texto a cada uno de los perfiles dados de alta en la aplicación.

b) La gestión de Inspecciones Oculares: Este módulo es el encargado de gestionar el alta, baja y modificación de las inspecciones oculares

c) La gestión de Evidencias: Este módulo es el encargado de gestionar el alta, baja y modificación de las evidencias asociadas a las inspecciones oculares

d) Análisis de datos en Cuadros de Mando Bussiness Intelligence: Este módulo presentará los Cuadros de Mando analíticos que explotarán los datos estadísticos relacionados con las inspecciones oculares realizadas, de cara a facilitar la identificación de patrones en los hechos analizados.

e) Administración: Este módulo es el encargado de gestionar los datos específicos de la aplicación como pueden ser la Gestion de Almacenes que albergan las evidencias, las tablas maestras (clave-valor) específicas de la aplicación. Además, se encargará de gestionar los turnos, citas, bajas, vacaciones de los agentes integrantes de los distintos grupos de las unidades de inspecciones oculares.

f) Migración de datos alojados en la actual aplicación ACCESS a la nueva aplicación objetivo de este contrato.

g) Exponer en el Servicio Horizontal de Codificaciones corporativo todos aquellos datos clave-valor que puedan ser susceptibles de ser utilizados por otras aplicaciones:

- Tipo Delito
- Marcas
- Tipo Lugar
- Modus
- Tipo Lugar
- Tipo Evidencia
- Tipo Resultado IP
- Compañías
- Estados de Solicitud

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS

La aplicación constará de 4 módulos

3.1. Área de Avisos

Este módulo es el encargado de gestionar los avisos generados en la aplicación. Otorga la capacidad de emitir mensajes de texto a cada uno de los perfiles dados de alta en la aplicación.

Estos mensajes disponen de vigencia y además del propio mensaje se informa el emisor, importancia y tipo de aviso.

3.1.1 Avisos:

Este sub módulo otorga las siguientes funcionalidades:

1. Emitir mensajes de texto a cada uno de los perfiles dados de alta en la aplicación.
2. Visualizar los mensajes destinados al usuario logado.

3.1.2 Gestión Avisos:

Permite la búsqueda, edición y supresión de avisos.

3.2. Área Inspecciones Oculares

A continuación, se describen los aspectos generales de las inspecciones oculares que servirá para percibir mejor el ámbito funcional a abordar.

La inspección ocular es la investigación de la escena de un hecho en sí mismo, siendo esta vital para su esclarecimiento. Esta pericia aporta una gran cantidad de información que posteriormente es tomada como prueba o indicio. En una inspección ocular se reúnen datos de personas, lugares, rastros, y todos los objetos que puedan ser de utilidad para descubrir la realidad de un hecho generalmente delictivo.

El objetivo de toda Inspección Ocular es el de hallar y preservar los indicios o evidencias que nos permitan obtener información de lo ocurrido en el lugar de los hechos, o acerca de las personas que allí estuvieron.

El Área de Inspecciones Oculares integra:

- La gestion de las propias Inspecciones Oculares
- La gestion de las evidencias asociadas a las inspecciones oculares
- La gestion de la ubicación o almacenaje de las evidencias

3.2.1 Gestión Inspecciones Oculares

Comprende la búsqueda, alta, baja y modificación de las inspecciones oculares. Deberá integrarse con la aplicación EUSKARRI para obtener los datos de la actuación que requiere de una inspección ocular. Además, también deberá integrarse con la aplicación de gestión de atestados del SIP para que una vez definido el atestado se pueda asociar a la inspección ocular creada.

La información que recogerá la Inspección Ocular constará de:

- Datos Generales: Recoge los datos propios de la inspección ocular: Fechas, actuación, atestado, descripción, identificación de si requiere estudio por parte de la Policía Científica, …
- Hechos: Recoge los datos relacionados con los hechos.
- Resumen:
    - Descripción: Leve descripción de la inspección ocular en la que se indicarán aquellos aspectos que sean relevantes.
    - Fotografías relevantes de la inspección ocular: Fotografías que pueden o no ser evidencias pero que pueden ser relevantes para la inspección ocular
- Evidencias de la Inspección Ocular: Listado de evidencias de la Inspección Ocular
- Estudios de las evidencias de la inspección ocular. Listado de estudios solicitados para las evidencias de la inspección ocular junto con sus respectivos resultados si los poseen
- Observaciones: Notas de texto que los investigadores relacionadas con la inspección ocular
- Relaciones: Relaciones con otros Atestados

- Histórico de acciones realizadas sobre la inspección ocular. Todas las acciones realizadas sobre una inspección ocular deberán ser auditadas por la aplicación registrando el usuario y acción realizadas. Así mismo, deberán dejar rastro en el componente de auditoría, de cara a cumplimiento del Reglamento de Protección de Datos.

3.2.2 Gestión de Evidencias

Comprende la búsqueda, alta, baja y modificación de las evidencias de las inspecciones oculares. Deberá integrarse con el Sistema de Gestión de Información de Laboratorio (Laboratory Information Management System, por sus siglas en inglés). Esta integración se realizará a través del sistema SIP alojado en IBM Host z/Os.

La información que recogerá la evidencia entre otros datos, será: inspección Ocular a la que está asociada, atestado, tipo, descripción, fotografías, estudios, ubicación, ….

3.2.3 Ubicación de Evidencias

Modulo que gestionara el registro de la ubicación física de las evidencias y sus movimientos entre almacenes. Permitirá la búsqueda, alta de ubicación y registro de movimientos de las evidencias. La ubicación de la evidencia vendrá definida por: Almacén, Armario y Estantería / Zona.

A la hora de registrar un movimiento la aplicación dará la opción de generar un documento PDF a modo de resguardo de la entrega/recogida de la misma.

3.3. Área de Administración

En este punto se realizará la administración de la aplicación y constará de los siguientes apartados:

- Gestión de almacenes
- Administración Delegada
- Mantenimiento de Maestros
- Gestion Calendarios

3.3.1 Gestión de almacenes

Este módulo será el encargado de la búsqueda, alta, baja y modificación de los Almacenes en los que se ubican las evidencias gestionadas por la aplicación.

Un almacén estará compuesto por la siguiente información:

- Nombre del almacén
- Ubicación del almacén: La ubicación del almacén deberá ser seleccionable en el momento del alta del almacén y se obtendrá de las ubicaciones disponibles en el árbol organizativo del Departamento de Seguridad y registradas en LDAP.
- Observaciones
- Armarios

Un Armario estará compuesto por la siguiente información:

- Nombre del armario
- Observaciones
- Estanterías/Zonas

Una Estantería/Zona estará compuesta por la siguiente información:

- Nombre de la estantería o zona
- Observaciones

3.3.2 Administración Delegada

La aplicación dará la opción de navegar a la actual aplicación de Administración Delegada alojada en el actual portal de Gurenet. Será necesario adecuar esta aplicación para que pueda administrar los accesos a Inspecciones Oculares.

3.3.3 Mantenimiento de Maestros

La aplicación Gestión de Inspecciones Oculares otorgara la capacidad de gestionar todas aquellas tablas maestras utilizadas por la aplicación y que albergaran información de tipo clave-valor como, por ejemplo:

- Grupos Unidad.
- Tipos de Aviso.

- Estados de la inspección ocular.

3.3.4 Gestión calendarios

Dentro de la administración existirá un módulo encargado de gestionar los calendarios de todos los usuarios integrantes de las distintas unidades de Inspecciones Oculares de la Ertzaintza. Desde este módulo los usuarios con el acceso correspondiente tendrán la opción de crear/modificar/eliminar citas de calendario referentes a:

- Cursos de formación
- Turno asignado(mañana/tarde/noche)
- Bajas Laborales
- Vacaciones
- Permisos
- Juicios
- Refuerzos
- …

Este módulo contará con la funcionalidad de validar que todos los días definidos en el calendario tienen asignados, el número mínimo de agentes definidos en la administración en cada uno de los turnos. Además, será capaz de generar distintos informes resumen en formato Excel:

- Nº de juicios entre dos fechas dadas
- Recuento de horas trabajadas entre dos fechas dadas por cada miembro de la unidad.
- Recuento de refuerzos entre dos fechas dadas
- …

3.4. Área de Análisis IIOO

La nueva aplicación Gestión de Inspecciones Oculares deberá disponer de un subsistema de consulta de datos estadísticos relacionados con las inspecciones oculares identificados sobre el presente pliego. El subsistema deberá permitir acotar la información estadística a mostrar por:

- Ubicación de los hechos
- Modus
- …

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

Las tareas a realizar consistirán en:

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

3.5. Integración con aplicación de emergencias Euskarri

Cualquiera de las distintas inspecciones oculares que se deben realizar, llevan aparejados los datos provenientes de una actuación EUSKARRI. Por lo tanto, la aplicación deberá integrarse con ésta para obtener los datos referentes a la actuación

3.6. Integración con el Sistema de Información Policial (SIP)

Al igual que con las actuaciones Euskarri, la aplicación deberá integrarse con el Sistema de Información Policial, para obtener la información de los posibles atestados creados en dicho sistema y que requieren de una inspección ocular.

De forma análoga, la aplicación deberá integrarse con este sistema para gestionar los estudios solicitados y sus resultados.

3.7. Generación del informe de Inspección Ocular

Todas las tablas que se muestren en la aplicación Gestión de Inspecciones Oculares deberán ser exportables a formatos Excel y PDF. Además, se dará la opción de generar un informe que recoja toda la información de la Inspección Ocular junto con las evidencias. Será generado e implementado mediante la herramienta corporativa de reporting IBERDOK. Este informe será el que posteriormente sea susceptible de dejarse a disposición judicial si el caso lo requiere.

3.8. Consideraciones adicionales

El alcance del sistema contempla, además, los siguientes aspectos fundamentales que deberán ser llevados a cabo por el adjudicatario durante la prestación de sus servicios:

1. Afianzar el cambio tecnológico Java EE emprendido, integrando esta iniciativa con el resto de las iniciativas ya completadas.
2. Los sistemas deberán proporcionar un tiempo de respuesta adecuado, evitando las opciones de desarrollo que puedan producir retardos en el mismo. Así mismo, deberán procurar que el entorno de trabajo sea intuitivo, y sencillo para el usuario.
3. Mejorar la eficiencia de los sistemas aprovechando los recursos y servicios disponibles en el propio Departamento de Seguridad y otras administraciones.
4. Conseguir una modernización de la plataforma de trabajo obteniendo una evolución continua de los desarrollos e incrementando mayor potencial a las funcionalidades actuales.
5. Aprovechar las sinergias que puedan surgir entre los diferentes proyectos (Framework de ejecución, infraestructura, procesos, servicios reutilizables, etc.).
6. Potenciar la prestación de servicios on-line.
7. Garantizar la continuidad operativa y tecnológica de las aplicaciones permitiendo flexibilidad hacia nuevos requerimientos.
8. Centralizar los servicios hacia un punto único de acceso y evitar la utilización de diversos productos y tecnologías para un mismo fin.
9. Proteger el sistemas de posibles indisponibilidad y/o alertar en caso de que se produzcan

El nuevo sistema a construir objeto del pliego deberá contemplar las siguientes características básicas:

- **Seguridad:**
  Aquellos servicios expuestos y limitados por la seguridad restringirán el acceso en función del usuario conectado.
- **Multilingüismo:**
  La nueva aplicación de portal ha de contemplar la posibilidad de selección del idioma de navegación (euskera o castellano).
- **Accesibilidad:**
  La nueva aplicación de portal cumplirá con los estándares tecnológicos y los requerimientos de accesibilidad establecidos por la DGTSI.
- **Servicios:**
  La nueva aplicación de portal se integrará con los servicios horizontales definidos según necesidades del análisis (gestor documental, Iberdok, concurrencia, auditoría, NORA, correo…)
- **Usabilidad:**
  La nueva aplicación de portal deberá seguir la guía de estilos que se proporcione por la DGTSI.
- **Navegadores**
  Se deberá garantizar que sea accesibles desde el navegador Microsoft Edge.

El sistema se integrará en la nueva plataforma tecnológica con tecnología Java EE. Dispondrá de una interfaz gráfica que se incorporará al portal de la intranet corporativa y proveerá de los servicios necesarios para resolver las peticiones y respuestas a las aplicaciones.

4. EJECUCIÓN DEL CONTRATO

4.1. Planificación y organización

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

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

4.2. Entorno tecnológico

La solución a los requerimientos recogidos en el presente pliego ha de ir alineada con la política de la DGTSI en lo que a desarrollos Java EE hace referencia.

La DGTSI proporcionara a la empresa adjudicataria toda la información necesaria para el desarrollo de este pliego en el nuevo entorno tecnológico.

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

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

Se deberá garantizar que la aplicación dentro de la intranet pueda ser accesible desde el navegador Microsoft Edge.

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

Gestión de portales y Servidor de aplicaciones:

- Desarrollo de Portlets sobre JBoss 7.3 y Liferay DXP 7.3
- Desarrollo de EJBs sobre Oracle WebLogic Server 12.2.1.4

Desarrollo de Portlets y EJBs sobre Liferay y Weblogic

- Portlet 3.0 (JSR-362)
- Java Server Faces 2.2
- Primefaces 8.0
- EJB 3.X + JPA 2.X
- OSGi R6 bundles
- Liferay MVC Portlet

Middleware de intercambio de información

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

Automatización de Procesos

- Control-M
- Apache Ant

Gestión documental

- IBM DB2 Content Manager v8.5

Frameworks y estándares:

- Todos los desarrollos deben realizarse para la versión 8 de la JDK
- Framework Bidea, GIDA.

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

Servidor de Bases de datos

- DB2 z/OS v.12
- Oracle 12c

Repositorio de código fuente

- Azure DevOps Server 2019

Repositorio Documental de Proyecto

- Microsoft SharePoint 2016.

Informes

- Herramienta de análisis de la información empresarial Microstrategy versión 2020, con especial funcionalidad en los módulos:
    - Developer
    - Microstrategy Web
    - Microstrategy Library
    - Embedding SDK
- Bases de Datos:
    - DB2 11.5 con Acelerador BLU
    - Ficheros planos
- Herramienta ETL: IBM InfoSphere DataStage es la 11.7.1.1

4.3. Cualificación técnica del equipo de trabajo

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

Jefe de Proyecto

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

Analista / Desarrollador

- Elaboración de las especificaciones técnicas de la solución así como preparación de su despliegue en los entornos del Departamento de Seguridad.
- Llevarán a cabo las tareas de desarrollo y construcción de las funcionalidades necesarias para la gestión de las inspecciones oculares.
- Preparación técnica y documental de los paquetes de versión necesarios para la implantación de las versiones necesarias.

4.4. Gestión de la calidad

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

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

- Controles de calidad para los entregables (documentación) que se hayan visto afectados.
- Pruebas unitarias que evite la introducción de un nuevo defecto al intentar reparar el inicialmente o la reparación incorrecta del error que se pretendía corregir.
- Pruebas de integración. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.
- Pruebas de sistema. Se ejecutarán para los módulos reparados y para todos aquellos que dependan directa o indirectamente de ellos.
- Pruebas de carga o rendimiento, en los casos, que se establezcan en función de la modificación realizada.
- Realización de los test de calidad, así como solicitud de la auditoría de calidad al equipo de la DGTSI encargado de dicha tarea.

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

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

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

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

- Fase gestión
    - Planificación y seguimiento del proyecto haciendo uso de las herramientas y plantillas de gestión definidas por normativa.
- Fase funcional
    - Documento de requisitos con la identificación de los requisitos funcionales/no funcionales del Sistema.
    - Análisis funcional con la descripción funcional del sistema e identificación de los procesos.
    - Casos de Uso con la definición de las secuencias de interacciones (pasos/actividades) que deberán realizarse para llevar a cabo entre los procesos del sistema y sus actores.
- Fase técnica
    - Arquitectura del sistema con el diseño a de la arquitectura y descripción de los componentes de la arquitectura junto sus relaciones.
    - Diseño físico de datos con el esquema físico de la base de datos y descripción de los objetos utilizados.
    - Volumetría del volumen estimado de las tablas e índices de BBDD.
    - Interface de usuario con el diseño de los interfaces de usuario necesarios para el sistema.
    - Plan de Pruebas con la relación de los casos de prueba, descripción de los pasos y resultados esperados.
    - Migración y carga Inicial, identificando los procesos necesarios para la migración de datos y/o cargas iniciales.

- Análisis de clases identificando las entidades para cada subsistema, especificando las responsabilidades que tienen asociadas, sus atributos y las relaciones entre ellas.

- Fase Implantación
  - Manuales de usuario según perfil.
  - Manuales de uso, aplicados a los servicios, en caso de que se defina alguno
  - Manual de explotación que recogerá el conjunto de tareas que se deberán realizar para la correcta explotación del sistema.

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

4.5. 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 el lugar de 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.

DOCUMENTOS ANEXOS

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

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

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

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

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

1 Acceso y protección de datos

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

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

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

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

(1) *Normativa: Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Directiva (UE) 2016/680 del Parlamento Europeo y Del Consejo de 27 de abril*

de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

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

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

2 Requisitos a cumplir para el desempeño en teletrabajo

Requisitos generales

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

Requisitos de los equipos

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

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

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

Requisitos de los usuarios

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

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

3 Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán a la Administración. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito de la Administración.

Asimismo, todos los entregables que deban facilitarse a los Departamentos y Organismos Autónomos del Gobierno Vasco (salvo las ofertas previas) únicamente deberán llevar como logotipo o señas de identidad el escudo del Gobierno Vasco o logotipos aceptados por el propio Departamento y Organismo Autónomo.

La empresa adjudicataria se verá también obligada a guardar las normas vigentes sobre, Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vea obligado a manejar.