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

EBA (ETXEKOEN ETA EMAKUMEEN BABESA)
2. FASEA

GESTIÓN DE EXPEDIENTES DE VIOLENCIA DOMÉSTICA Y DE GÉNERO DE EUSKADI
FASE 2

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 4

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS. 5

3.1. INTERCOMUNICACIÓN CON VIOGEN 5
3.2. NUEVAS FUNCIONALIDADES EN SISTEMA EBA 6
3.3. OPTIMIZACIÓN DE PROCESOS EN EL SISTEMA EBA 7
3.4. ADAPTACIÓN DEL SISTEMA EBA A LA NUEVA PLATAFORMA TECNOLÓGICA CORPORATIVA 8
3.5. SISTEMA EBA EN GURENET PARA ERTZAINTZA 9
3.6. SOPORTE PARA EL MANTENIMIENTO DEL SISTEMA 9
3.7. CARACTERÍSTICAS BÁSICAS 10

4. EJECUCIÓN DEL CONTRATO 11

4.1. PLANIFICACIÓN Y ORGANIZACIÓN 11
4.2. ENTORNO TECNOLÓGICO 11
4.3. CUALIFICACIÓN TÉCNICA DEL EQUIPO DE TRABAJO 13
4.4. GESTIÓN DE LA CALIDAD 14
4.5. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN 16
4.6. REGISTROS, NOTIFICACIONES E INVENTARIOS. 16
4.7. LUGAR DE EJECUCIÓN DEL CONTRATO. 17

DOCUMENTOS ANEXOS 18

ANEXO 1. NORMAS DE SEGURIDAD RELATIVAS A LOS SISTEMAS DE INFORMACIÓN. 18

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 el marco de la estrategia de transformación digital, todas las cuestiones referentes a la planificación, elaboración, desarrollo y ejecución, así como la gestión y mantenimiento de los destinados a actividades de seguridad pública, por lo que en virtud de dicha competencia se acomete el presente expediente.

La legislación de aplicación en la materia (Leyes de Policía del País Vasco y de Ordenación del Sistema de Seguridad Pública de Euskadi) impulsa el concepto de Policía del País Vasco, conformada por la Ertzaintza y las Policías Locales. Con el fin de seguir avanzando en la coordinación operativa y de sistemas de información entre la Ertzaintza y las Policías Locales, surge la necesidad de incorporar nuevas funcionalidades y mejoras al proyecto EBA (Etxekoen eta Emakumeen Babesa) que da cabida al tratamiento de la violencia doméstica y/o de género vasco, con gestión compartida por parte de las policías locales y de la Ertzaintza, para facilitar la toma de decisiones y minimizar los riesgos de sufrir nuevos episodios de violencia por parte de las víctimas.

Para ello, una vez puesto en funcionamiento dicho proyecto, se recoge la necesidad de incorporar nueva funcionalidad a la aplicación, de cara a poder completar el procedimiento de gestión y seguimiento de expedientes EBA. Adicionalmente, se quiere intercomunicar con la plataforma de expedientes de violencia doméstica y de género estatal, VIOGEN, tanto para que el sistema EBA pueda consultar expedientes VIOGEN, como para permitir al sistema VIOGEN consultar los expedientes de la Policía Vasca. Por último, se precisa de desarrollos de optimización de algunos procesos implementados ya en la plataforma EBA, surgidos de su puesta en funcionamiento, junto con la adaptación de los desarrollos ya realizados a las nuevas plataformas tecnológicas corporativas. Por último, se precisa de la implementación de la consulta del sistema EBA en la intranet corporativa Gurenet de modo que se facilite la consulta de dichos expedientes desde la mencionada plataforma.

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

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 segunda fase del sistema informático EBA (Etxekoen eta Emakumeen Babesa) para la Gestión de expedientes de Violencia Doméstica y de Género de Euskadi. Esta fase contempla las siguientes necesidades surgidas tras la puesta en funcionamiento del sistema EBA:

a) Intercomunicación con la plataforma de expedientes de violencia doméstica y de género estatal, VIOGEN, tanto para que el sistema EBA pueda consultar expedientes VIOGEN, como para permitir al sistema VIOGEN consultar los expedientes de la Policía Vasca.

b) Incorporación de nuevas funcionalidades de gestión y seguimiento de expedientes de Violencia Doméstica y de Género dentro del portal de Udaltzaingoa privado.

c) Optimización de procesos ya implementados en la plataforma EBA para facilitar la tramitación de los expedientes EBA.

d) Adaptación de los desarrollos ya realizados en el sistema EBA a la nueva plataforma tecnológica corporativa del portal de Udaltzaingoa privado.

e) Desarrollar la consulta de expedientes EBA desde Gurenet para Ertzaintza.

Las necesidades identificadas anteriormente constituyen módulos funcionales susceptibles de ser implantados de forma independiente y escalados en el tiempo. Es necesario establecer un soporte post-implantación que consistirá en realizar las labores de mantenimiento correctivo y evolutivo que permita dar respuesta a las necesidades de las diferentes policías locales a medida que vayan utilizando dicho sistema, se vayan incorporando nuevas policías al mismo o surjan nuevas necesidades de interconexión con sistemas ajenos al Departamento.

Antes de abordar el 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 PPT.

3. DESCRIPCIÓN DE LAS FUNCIONALIDADES REQUERIDAS.

3.1. Intercomunicación con VIOGEN

La Junta de Seguridad toma nota y aprueba el acuerdo alcanzado en el seno de la Comisión Permanente de Coordinación celebrada el pasado 12 de mayo, por el que se adquiere el compromiso de interconectar los respectivos sistemas de seguimiento de casos de violencia de género entre la Secretaría de Estado de Seguridad de España y el Departamento de Seguridad del Gobierno Vasco.

De acuerdo con este compromiso, se precisa de las tareas necesarias para implementar la intercomunicación con la plataforma de expedientes de violencia doméstica y de género estatal, VIOGEN, tanto para que el sistema EBA pueda consultar expedientes VIOGEN, como para permitir al sistema VIOGEN consultar los expedientes de la policía vasca. Dentro de las tareas a desarrollar, se encuentran las siguientes:

- Desarrollar la implementación de la consulta a los servicios de búsqueda de personas y búsqueda de casos publicados por el sistema VIOGEN
- Configurar la respuesta recibida de los servicios de búsqueda de personas y búsqueda de casos del sistema VIOGEN para su utilización en el sistema EBA del portal de Udaltzaingoa y en el sistema EBA de la Ertzaintza.
- Implementar la utilización de los servicios de búsqueda de personas y búsqueda de casos del sistema VIOGEN dentro del sistema EBA del portal de Udaltzaingoa.
- Desarrollar la implementación de dos nuevos servicios web de búsqueda de personas y búsqueda de casos en el sistema EBA
- Realizar las tareas y mecanismos de configuración y publicación de los servicios web de búsqueda de personas y búsqueda de casos del sistema EBA para dejarlos accesibles a la Secretaría de Estado de Seguridad de España para su consumo

3.2. Nuevas funcionalidades en sistema EBA

Dentro de los procedimientos de gestión y tramitación de los expedientes de violencia y de género de la Policía Vasca hay recogidas ciertas tareas que actualmente el sistema EBA del portal de Udaltzaingoa no las contempla. Para que todas las policías que componen el sistema EBA funcionen igual, se precisa de la implementación de los siguientes requerimientos dentro del sistema EBA del portal de Udaltzaingoa:

- Añadir en la carátula del Expediente:
  - Víctima protegida mediante pulsera telemática
  - Orden de Protección y con qué medida de alejamiento y adjuntos
  - Protección con escolta
- Notificación de Udaltzaingoa a Ertzaintza para realizar preventivas y viceversa, es decir, recepción de notificaciones de Ertzaintza a Udaltzaingoa para realizar preventivas.
- Transferencia de expedientes de Ertzaintza a Udaltzaingoa con previo aviso de la solicitud de transferencia y aceptación por parte de Udaltzaingoa
- Incluir Vehículos de la Víctima y el Autor en pantalla y en la Ficha Víctima
- Gestión de personas con acceso restringido
- Nuevos perfiles para dar autorizaciones
- Implementar un procedimiento para registrar las entrevistas
- Implementar un procedimiento para registrar las rutinas
- Visualizar los correos que se han enviado desde Udaltzaingoa asociados a un expediente
- Implementar un procedimiento para registrar las agendas de acontecimientos
- Implementar un procedimiento para registrar los teléfonos Bortxa
- Añadir pautas de actuación específicas por víctima y mostrarlas también en carátula
- Añadir un indicador de riesgo de exclusión

- Añadir valoración para menores por convivencia
- Añadir informe general y análisis, junto con el resumen del expediente
- Incorporar datos físicos de las personas
- Incorporar el consentimiento de cesión de datos para Servicios Sociales en cada víctima y mostrarlo también en carátula
- Incorporar y visualizar más de una foto para la persona que se está introduciendo
- Poder asociar más de una identificación por persona
- Implementar un procedimiento de borrado de expedientes, valoraciones e identificación de persona
- Adjuntar y ver más de un documento en un apunte

3.3. Optimización de procesos en el sistema EBA

Una vez implementada la primera fase del sistema EBA y tras su puesta en funcionamiento, se han recogido un conjunto de requerimientos de optimización de su utilización, de cara a facilitar las tareas de registro y seguimiento de expedientes EBA, así como la comprensión del sistema. Estas tareas serán tanto de carácter visual como funcional.

Dentro de los requerimientos recogidos, se encuentran, entre otros, los siguientes:

- Permitir el registro de domicilios fuera del Estado para las personas involucradas en los expedientes EBA.
- Modificar la visualización de la pantalla de listados apuntes-valoraciones
- Permitir introducir la referencia de la orden judicial del juzgado, junto con otras referencias de atestados e incidencias propias de cada Udaltzaingoa
- Visualizar el listado de estudios vicarios en otra lista
- Permitir modificar un apunte que ya ha sido valorado
- Permitir adjuntar otro tipo de documentos que no sean PDFs
- Incorporar la identificación de personas dentro de otros expedientes EBA por su nombre y/o apellidos

- Transferir automáticamente un expediente con titularidad Udaltzaingoa y referencia Ertzaintza, que se encuentre cerrado antes de la migración inicial, al reabrirlo.
- Permitir añadir apuntes en expedientes no titulares que estén cerrados
- Permitir modificar apuntes de otra policía en un expediente del que se es titular
- Poder ver la fecha de alta/modificación de un domicilio en pantalla
- Enlazar con los documentos recogidos en los apuntes de la Ertzaintza
- Permitir añadir apuntes en un expediente del que no se es titular cuando la relación todavía no existe
- Añadir parámetros de búsqueda dentro del listado de apuntes.
- Mejora de las búsquedas por persona
- Otras mejoras del sistema ya implementado que se vayan recogiendo a lo largo de las sesiones de soporte realizadas con Ertzaintza y Udaltzaingoa.

3.4. Adaptación del sistema EBA a la nueva plataforma tecnológica corporativa

El portal de Udaltzaingoa está en proceso de adaptación a la nueva plataforma tecnológica corporativa Liferay. Con objeto de que los desarrollos ya implementados en la primera fase del sistema EBA mediante la tecnología anterior se integren dentro de la nueva plataforma tecnológica, se precisa la migración de la capa de presentación del sistema EBA a esta nueva tecnología y su adaptación a la capa de negocio y seguridad. Las tareas de migración consisten básicamente en:

- Adaptar la capa de presentación del sistema EBA ya implementado a Liferay
- Amoldar los desarrollos de negocio para publicar los EJBs que se consuman desde presentación como servicios web SOAP
- Incorporar los elementos de seguridad necesarios en las operaciones de negocio que exijan identificación de usuario

3.5. Sistema EBA en Gurenet para Ertzaintza

Actualmente el tratamiento del sistema EBA desde el entorno web sólo está accesible para Udaltzaingoa. De cara a que la Ertzaintza pueda visualizar los expedientes EBA desde un entorno web, se precisa de la implementación del sistema EBA dentro de la intranet corporativa Gurenet. Este sistema será un reflejo del sistema EBA de Udaltzaingoa con la particularidad de que será únicamente en modo consulta. No se permitirá realizar modificaciones sobre él. La visualización de los expedientes de los que la Ertzaintza no es titular, tendrá las mismas características y restricciones de visualización que Udaltzaingoa tiene para los expedientes de los que no son titulares.

3.6. Soporte para el mantenimiento del sistema

Mediante este soporte se precisa atender las dudas de uso de aplicación que puedan tener las diferentes policías locales. Para ello, se realizarán jornadas periódicas de soporte en las que se explicará cómo gestionar determinadas cuestiones. A estas jornadas acudirán también los gestores funcionales de manera que se pueden atender tanto las cuestiones de procedimiento como técnicas. Además, durante estas sesiones es habitual detectar incidencias que deben ser corregidas, así como aspectos de mejora, que tras aprobación por los gestores funcionales deben ser incorporadas al sistema lo antes posible.

Adicionalmente, se prevén futuras nuevas interconexiones con terceros, de las que actualmente no se conocen los requerimientos, pero que una vez definidos, deben abordarse e integrarse en esta plataforma.

Todas estas cuestiones serán cubiertas a través de este nivel de soporte que se establece según las necesidades detectadas conforme vayan implantándose los diferentes módulos de la fase II del proyecto.

3.7. Características básicas

El 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 aplicación de portal ha de contemplar la posibilidad de selección del idioma de navegación (Euskera o Castellano)
- **Accesibilidad:**
  La aplicación de portal cumplirá con los estándares tecnológicos y los requerimientos de accesibilidad establecidos por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.
- **Servicios:**
  La aplicación de portal se integrará con los servicios horizontales definidos según necesidades del análisis (gestor documental, auditoría, correo, …).
- **Usabilidad:**
  La nueva aplicación de portal deberá seguir la guía de estilos que se proporcione por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos y ser responsive.
- **Adaptabilidad:**
  Las nuevas funcionalidades se adaptarán al tratamiento y diseño de dichas funcionalidades en el sistema EBA ya implementado.
- **Navegadores:**
  Se deberá garantizar que sea accesible desde los navegadores basados en Chromium versiones 98 o superiores, en concreto con los navegadores Google Chrome y Microsoft Edge.

El sistema respetará la interfaz gráfica y los estilos de los portales tanto de Udaltzaingoa como Gurenet 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 que intervendrán en la ejecución del contrato. Asimismo, deberá presentar el correspondiente diagrama temporal de actividades (cronograma de tareas).

La correcta planificación y organización van a ser las estrategias que permitan distribuir el tiempo disponible de la forma más racional posible, permitiendo el correcto ajuste temporal de todas las tareas que constituyen el contrato.

Para las tareas de soporte post-implantación, se deberá identificar la forma en que se prevé llevar a cabo las mismas, con indicación de los recursos a asignar.

4.2. 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 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 “Udaltzaingoa”.

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 parte privada de Udaltzaingoa pueda ser accesible desde los navegadores basados en Chromium versiones 98 o superiores.

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

- Liferay DXP 7.3+ JBoss 7.4
- IBM WebSphere Application Server v8.5
- Desarrollo de Portlets y EJBs sobre Liferay y WAS 8.5
    - Portlet 3.0 (JSR-286)
    - Java Server Faces 2.2 (PrimeFaces 8)
    - EJB 3.2 + JPA 2.1
    - OSGi R6 bundles

Gestión documental

- IBM DB2 Content Manager v8.5

Mensajería JMS/MQ

- IBM Websphere MQ 7.5

Bus de integración de servicios y aplicaciones

- Oracle Service Bus 12c

Servidor de Bases de datos

- DB2 z/OS v.12

Automatización de procesos

- Control-M

Repositorio de código fuente

- Azure DevOps Server 2020

Repositorio Documental de Proyecto

- Microsoft SharePoint 2016

Frameworks y estándares

- Librerías internas "GIDA" para funcionalidades comunes: trazas de aplicación, consulta de propiedades, credenciales de usuario, etc.
- La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos dispone de un conjunto de servicios horizontales y componentes reutilizables para dar solución a las necesidades comunes identificadas por las aplicaciones.

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 de las tareas de análisis y diseño de la arquitectura funcional y tecnológica de la solución, así como de definir su configuración y despliegue.
- Será el soporte técnico de alto nivel para todo el equipo de trabajo, sobre la plataforma, orientando las soluciones óptimas a las necesidades que puedan plantearse, tanto desde el punto de vista técnico como funcional.
- Colaboración con el equipo de la 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.

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 Dirección de Gestión 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 el Plan de Calidad del Departamento de Seguridad. Entre los aspectos a contemplar estarán los siguientes:

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

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

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

El número de 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 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

- Fase Implantación
  - Manuales de usuario según perfil
  - Manual de explotación que recogerá el conjunto de tareas que se deberán realizar para la correcta explotación del sistema.

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 de la Dirección General de Telecomunicaciones y Sistemas Informáticos.

La empresa adjudicataria deberá proporcionar la información requerida por la Dirección General de Telecomunicaciones y Sistemas Informáticos para conocer la situación y desarrollo de la ejecución del contrato. Esta información se proporcionará en forma de informes que deberán presentarse de forma periódica.

La elaboración de estos informes periódicos tiene carácter obligatorio y será entregado al técnico o técnica responsable de la Dirección General de Telecomunicaciones y Sistemas Informáticos.

4.7. Lugar de ejecución del contrato.

El lugar de trabajo, por defecto, serán las instalaciones que determine y disponga la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos en su sede de Larrauri Mendotxe bidea, 18 en Erandio (Bizkaia), si bien se podrán establecer porcentajes de teletrabajo para la realización de las tareas recogidas en este P.P.T.

DOCUMENTOS ANEXOS

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

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

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

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

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

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

1 Acceso y protección de datos

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

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

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

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

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

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

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

2 Requisitos a cumplir para el desempeño en teletrabajo

Requisitos generales

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

Requisitos de los equipos

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

- Los equipos se utilizarán exclusivamente con fines laborales y para tal fin serán proporcionados por la empresa adjudicataria del contrato de servicios.
- Para el acceso a internet se utilizarán redes seguras, entendiéndose como seguras las redes que sean gestionadas por el usuario (red doméstica) o su empresa.
- Los equipos contarán con un lector de tarjetas digitales para la autenticación del usuario.
- Los equipos contarán con un dispositivo TPM2.0.
- El sistema operativo será Microsoft Windows, en versiones soportadas y con licencia oficial de Windows 10 o superior.
- Los discos locales estarán cifrados con BitLocker.
- Se aplicarán las actualizaciones recomendadas por el fabricante del sistema operativo con una periodicidad no superior a 60 días.
- El equipo tendrá instalado y operativo un software EPP o EDR actualizado diariamente.
- Se remitirá por cada equipo un listado del software adicional instalado, incluyendo versiones, para su autorización expresa por el Departamento de Seguridad.
- La BIOS del dispositivo estará protegida por una contraseña robusta.

Requisitos de los usuarios

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

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

3 Propiedad intelectual

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

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

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