Departamento de Seguridad del Gobierno Vasco

# Evolución del Sistema Identificación Biométrica, MorphoBis

Pliego de Bases Técnicas

Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos

# Índice

1 Introducción ..... 2
1.1 Justificación de la necesidad ..... 2
2 Objeto ..... 3
3 Descripción detallada del servicio. ..... 4
3.1 Descripción del servicio a ofertar. ..... 4
3.1.1 Integración de Policías Locales ..... 4
3.1.2 Intercomunicación con Avantius ..... 5
3.1.3 Mejoras en Usabilidad ..... 5
3.2 Instalación ..... 6
3.3 Documentación ..... 7
4 Condiciones de garantía y mantenimiento ..... 8
5 Condiciones generales de ejecución ..... 9
5.1 Equipo de trabajo. ..... 9
5.2 Jornada Laboral. ..... 9
5.3 Seguimiento y control. ..... 9
6 Condiciones de seguridad. ..... 10

# 1 Introducción

## 1.1 Justificación de la necesidad

El Departamento de Seguridad del Gobierno Vasco renovó el Sistema Automatizado de Identificación de Huellas Dactilares (AFIS) de la Ertzaintza, mediante el expediente E0030/2020 "Actualización de sistema de Identificación Biométrica". Dicho expediente fue adjudicado a la empresa IDEMIA Identity & Security France S.A.S. por el procedimiento negociado sin publicidad.

El contrato supuso la puesta en marcha del software MorphoBis versión 5.7, la adquisición de estaciones MESA, de tablets MIMS, de software de identificación para equipos Windows y de la plataforma Face Expert 3.1.0.2.

La integración con las herramientas del Sistema de Informática Policial se ha hecho mediante el diseño de la interoperabilidad con el sistema UXUE.

En el periodo transcurrido desde la puesta en marcha del sistema, se han producido varias cuestiones que no habían sido contempladas en el expediente E0030/2020, y que deben ser implementadas sin demora en la plataforma de identificación biométrica, MorphoBis.

Así, el Plan General de Seguridad Pública de Euskadi establece dentro de sus líneas estratégicas, el compromiso de alcanzar una seguridad integral e interconectada, para lo cual se han de potenciar mecanismos de coordinación y cooperación entre Ertzaintza y Policías Locales, para hacer realidad una Policía del País Vasco corresponsable y eficiente. En este sentido, se requiere la incorporación de las Policías Locales en el sistema de Identificación Biométrica de la Ertzaintza, MorphoBis

De este mismo compromiso se deriva en la necesidad de comunicar el Sistema de Identificación Biométrica, MorphoBis, con el Sistema de Gestión Procesal AVANTIUS puesto en marcha por la Administración de Justicia.

Además, la experiencia adquirida por las personas usuarias del sistema MorphoBis, desde su puesta en marcha, ha permitido detectar algunos aspectos cuya implementación supondrá una importante mejoría en la usabilidad del sistema.

# 2 Objeto

El objeto de este expediente es proporcionar al Departamento de Seguridad del Gobierno Vasco (DSGV) la mejora del actual sistema MorphoBis versión 5.7, en cuanto a la incorporación de las Policías Locales al sistema de Identificación Biométrica de la Ertzaintza, la integración de MorphoBis con el Sistema de Gestión Procesal AVANTIUS, y la mejora de la usabilidad del sistema.

# 3 Descripción detallada del servicio.

## 3.1 Descripción del servicio a ofertar.

Los trabajos a realizar sobre el sistema implantado se dividen en tres grandes grupos:

- **Integración en el sistema de las Policias Locales** con el objetivo de potenciar los mecanismos de coordinación y cooperación entre Ertzaintza y Polícias Locales.
- Incorporación de sistemas automáticos que faciliten la comunicación recopilada bajo el Sistema de Identificación Biométrica Morphobis con el Sistema de Gestión Procesal **Avantius**.
- **Mejora en la usabilidad**, incorporando información adicional en los elementos que se interconectan con sistemas policiales y que mejorarán la interacción de las personas con este nuevo sistema.

Previo al inicio de cada uno de los tres grupos de trabajo, deberá contemplarse realizar las reuniones de análisis y diseño técnico necesario que permita resolver las casuísticas de detalle sobre las que tienen afectación.

### 3.1.1 Integración de Policías Locales

El Plan General de Seguridad Pública de Euskadi establece dentro de sus líneas estratégicas, el compromiso de alcanzar una seguridad integral e interconectada, para lo cual se han de potenciar mecanismos de coordinación y cooperación entre Ertzaintza y Policías Locales, para hacer realidad una Policía del País Vasco corresponsable y eficiente.

En este sentido, se debe adecuar el sistema de Identificación Biométrica de la Ertzaintza MorphoBis para que las Policías Locales que adquieran el sistema de MESA de IDEMIA pueda conectarse al sistema de la Ertzaintza.

El sistema de identificación de las MESAS deberá permitir incluir usuarios/contraseñas Udaltzaingoak que residen en el sistema de identificación de Ertzaintza (ActiveDirectory) categorizados como Udaltzaingoak. Este usuario, alfanumérico, no sigue el mismo formato que actualmente tienen los y las agentes de Ertzaintza. El formato será 3 dígitos + 1 letra + 4 dígitos. La configuración del ActiveDirectory será responsabilidad del Departamento de Seguridad, siendo IDEMIA la encargada de ajustar el sistema de identificación actual para permitir ese grupo de usuarios.

La MESA deberá realizar la identificación de usuario y contraseña contra la rama correspondiente a Udaltzaingoak.

La información del usuario identificado deberá distribuirse en todas las comunicaciones que MBIS realiza con los sistemas que se interconecta (como por ejemplo UXUE) así como almacenar en su modelo de datos toda la auditoria y datos que cada Udaltzaingoak realiza.

Previo a abordar este cambio se realizará una reunión de análisis que permita identificar los puntos del sistema actual que se ven afectados en esta nueva evolución, identificando también en qué puntos de integración deberá revisarse el formato del envío de usuario que se realiza en la actualidad.

### 3.1.2 Intercomunicación con Avantius

La Administración de Justicia ha puesto en marcha recientemente el Sistema de Gestión Procesal AVANTIUS. En la actualidad el Sistema de Información Policial ya realiza envíos automáticos de la información que se recogen en Diligencias y Atestados de actuaciones policiales. Como parte de esta información debe remitirse la información biométrica recogida en el nuevo sistema Morphobis.

Con la intención de automatizar este envío de información se requiere habilitar un servicio web, siguiendo la estructura de API de interconexión que ya existe entre MBIS – UXUE. Este nuevo servicio, denominado TPCard, que genere el PDF que actualmente genera el sistema MBIS. Los parámetros de este servicio serán:

- PIN / Tipo Identificación / Referencia (sólo por PIN, o por los tres)
- Online SI/NO. Esto significa
    - Online = SI es que la TPCard es devuelta por el propio servicio, en Base64.
    - Online=NO significa que la TPCard en formato PDF se guarda en un directorio al que tiene acceso MBIS que se especifica en el parámetro directory. Ese directorio estará compartido entre el sistema MBIS y los sistemas UXUE y SIP.
- directory. Contendrá la ruta absoluta del directorio en el que MBIS generará la TPCard (sólo se tendrá en cuenta cuando Online=SI).

Durante el proyecto se analizará en detalle este servicio para definir los códigos de error que este servicio deberá contemplar.

Además, se revisará la generación de TPCard, tanto a través de este nuevo servicio web como a través de la interfaz de MBIS, MESA y MIMS, para validar que los datos alfanuméricos deban ser proporcionados por UXUE y no por MESA. Sólo serán alimentados por MBIS cuando no estén alojados en UXUE.

Se realizarán pruebas de integración y aceptación del servicio web y de la evolución de la generación de la TPCard con el sistema UXUE.

### 3.1.3 Mejoras en Usabilidad

Tras la puesta en marcha del nuevo sistema MorphoBis se han identificado ciertas situaciones de tratamiento de datos que requieren una evolución en la gestión del sistema que facilite la labor de introducción de datos a la persona usuaria:

- Se revisarán la gestión de errores de la integración con UXUE tanto desde MorphoBis, MESA, Surface Pro y MIMS. Se trata de recuperar los códigos de error identificados en

la interfaz de comunicación y presentar un mensaje entendible y sencillo a la persona usuaria.

- Número y tipo de documento. Obligatorio en la adquisición de datos. Sólo en tipos de identificación "Indocumentado" estos dos valores pueden estar vacíos. Deberá aplicarse la evolución tanto en MESA, MBIS y MIMS.
- Filtro de búsqueda de "Referencia Policial". Incluir la Referencia Policial como filtro en el explorador de casos MLE. Se incorporará debajo del filtro "ID" para que los operadores puedan filtrar sobre la referencia.
- Dosieres sin fotos. En MESA cuando se un operador vaya a enviar un expediente al sistema central sin validar la captura de retratos que ha realizado se incluirá un mensaje de aviso. "Está a punto de enviar un expediente al sistema central sin haber validado la captura de retratos. Haga click en el botón "Cancelar" para volver atrás y validar la captura de retratos o haga click en el botón "Finalizar" para enviar el expediente sin retratos"
- Gestión de los casos criminales "Case ID". La identificación de casos MIMS deberán cambiar el formato, ya que los identificadores de casos son administrados por el sistema central y los operadores de campo no conocen la identificación de casos. Para esto se modificará el formato de casos en MIMS pasando de ser YYYYxxnnnnn por MIYYxxnnnnn (donde YY será el año, xx será un número del 01 al 17 para identificar a las MIMS, y nnnnn será un número correlativo). Este nuevo formato permite a MBIS poder diferencias los casos MiMs de los casos MLE. En el sistema MLE, al abrir un caso que tenga el formato de MiMs Case ID, se obligará al operador a cambiar por un ID de caso MLE estándar. Cuando se modifique este identificador, el sistema deberá cambiarlo en el ID del caso contenido en el descriptor de la persona asociada. Este cambio no afecta a MESA.
- Incluir la gestión de cambio automático S/N para los casos de uso CU002 y CU003 del sistema UXUE.
- Adecuar la información del PAIS destino en la solicitud de InterAfis a los últimos requisitos que marca el sistema PRUM. Deberán realizarse las pruebas de integración con el sistema en el que entre otros entes deberá coordinarse con Policía Nacional.
- Se debe garantizar, ante posibles errores en el hardware de MESA de una Ertzain-Etxea, habilitar el servicio con agilidad. Para esto se requiere un escáner de huellas para MESA (TP-5300A-HD W/O DIRECT FS (EMBALLE)) que sirva de repuesto antes este tipo de incidencias, mientras se repara el hardware original.

## 3.2 Instalación

La empresa adjudicataria realizará todas las labores de instalación y configuración pertinentes tanto en el entorno de TestBed como en el entorno de producción necesarias para la puesta en marcha de los desarrollos y evoluciones incluidos en el presente pliego. Deberá tenerse en cuenta que estas instalaciones y/o configuraciones pueden afectar a todos los componentes que forman el sistema MBIS como por ejemplo: sistemas centrales de servidor, puestos del experto, Line-UP, MESA, MIMS, Surface PRO.

Para que desde el Departamento de Seguridad se puedan realizar las labores de aceptación e integración, la empresa adjudicataria deberá realizar la preparación de datos en el entorno de TestBed que permita realizar las pruebas de aceptación y de integración que garanticen la puesta en marcha de las evoluciones en el sistema de Producción.

Para la implantación de estos cambios se estima la presencia del equipo de la empresa adjudicataria en las instalaciones del Departamento, de manera temporal, mínimo en 6 ocasiones.

## 3.3 Documentación

La empresa deberá entregar la documentación y los diferentes entregables y productos correspondientes a cada trabajo.

La documentación que deberá actualizarse en base a los cambios de este pliego se basan en la documentación que existe sobre el sistema. Deberá revisarse y actaulizarse aquella documentación afectada, siendo al menos esa revisión sobre:

- Documento de arquitectura del sistema, con el mayor detalle posible en cuanto a elementos, software licenciado y funcionalidades disponibles. Se incluirán, cuando proceda, datos físicos como consumo eléctrico, peso, disipación térmica, etc.
- Manual de procedimientos de administración de los sistemas incluyendo los scripts utilizados en cada caso.
- Procedimientos relacionados con la continuidad del servicio.
- Manuales de usuario que recojan las funcionalidades de cada uno de los elementos de captura y cotejo de datos.
- Plan de implantación con descripción y cronograma de las tareas y actividades previstas.
- Plan de mantenimiento de los equipos y aplicativos suministrados con el servicio.
- Descripción de los mecanismos de garantía y soporte incluyendo direcciones de correo, teléfonos de contacto, etc.

La documentación se entregará de forma electrónica en el repositorio que indique la DGTSI. Estará cumplimentada en, por lo menos uno de los dos idiomas oficiales de la CAPV. Como excepción, los informes de seguimiento se entregarán también en soporte papel. La DGTSI se reserva el derecho a solicitar que toda la documentación se entregue también en soporte papel.

Los manuales de usuario se entregarán en Castellano. Los manuales de usuario actualizados tendrán una tabla que permitirá al usuario identificar los cambios con su versión anterior, y así poder identificar de manera rápida las nuevas funcionalidades y su funcionamiento, facilitando la adquisición de conocimientos.

Además, como resultado del proyecto se obtendrán los binarios y ejecutables, instalados en el entorno de producción, probados y validados.

Todos los entregables deberán tener la calidad técnica exigible y entregarse en el plazo establecido en el proyecto.

No se considerará finalizado el proyecto hasta que toda la documentación se encuentre a disposición del Departamento de Seguridad y sea validada por personal técnico del mismo.

# 4 Condiciones de garantía y mantenimiento

Una vez completa la fase de instalación de los sistemas el sistema nuevo se considerará productivo y, por lo tanto, recibirá un soporte que tendrá, al menos, los siguientes SLA:

- Hotline para consultas 24/7
- Soporte técnico en horario de 09:00 a 18:00 horas de acuerdo al calendario laborar del adjudicatario.

# 5 Condiciones generales de ejecución

## 5.1 Equipo de trabajo.

La empresa adjudicataria designará una persona que, como Jefe de Proyecto, tendrá la función de representante de la misma y de interlocutor y responsable de los trabajos ante la jefatura de la DGTSI. Su sustitución no podrá llevarse a cabo sin conformidad previa de la DGTSI.
Facilitará a las personas designadas por la DGTSI toda la información y documentación necesarias para tener en cada momento conocimiento preciso del estado del proyecto, de las circunstancias en las que se desarrollan los trabajos del mismo.
La comunicación y coordinación con la DGTSI deberá hacerse de forma permanente. A tal efecto, la DGTSI coordinará los trabajos disponiendo el siguiente equipo:

- El Jefe de Sección que actuará como coordinador del proyecto, marcará las directrices de los trabajos del proyecto. Estas directrices serán de obligado cumplimiento para el adjudicatario.
- Un equipo técnico formado por personas conocedoras de los distintos ámbitos de negocio del Departamento de Seguridad y de las tecnologías implicadas en el proyecto. La dedicación de este equipo se ajustará a las necesidades de cada momento.

## 5.2 Jornada Laboral.

Los trabajos que puntualmente se realicen en los locales del Departamento de Seguridad, de forma conjunta con técnicos o usuarios del mismo, se harán de forma adecuada a la jornada de trabajo establecida para los trabajadores del Departamento de Seguridad.

## 5.3 Seguimiento y control.

En el lanzamiento del proyecto se concretarán los procedimientos de seguimiento y control aplicados por la DGTSI en sus proyectos. Estos deberán ser cumplidos por la empresa.

En cualquier caso, la empresa deberá realizar un informe de seguimiento con la periodicidad acordada con la DGTSI y de los problemas que puedan encontrarse. De esta manera se buscarán las soluciones y herramientas precisas para cada situación.

# 6 Condiciones de seguridad.

El adjudicatario se compromete a cumplir la política de Seguridad de la Información del Departamento de Seguridad del Gobierno Vasco y todas las normativas y procedimientos aplicables en el contexto del servicio.

El Departamento de Seguridad del Gobierno Vasco tendrá derecho a llevar a cabo auditorías de las actividades del equipo de trabajo del adjudicatario para asegurarse de que la prestación de los servicios se realiza de acuerdo a lo establecido en el presente pliego. Todo el material e información requerida para dichas inspecciones estará disponible sin restricciones.

La información facilitada para abordar los trabajos no se aplicará ni utilizará con una finalidad diferente a la que es objeto de este pliego ni el prestador del servicio la comunicará, ni siquiera a efectos de su conservación a terceros.

El adjudicatario y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del servicio prestado.

El adjudicatario deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Al finalizar el contrato, y una vez haya sido transferida la información al Departamento de Seguridad del Gobierno Vasco, el adjudicatario se compromete a destruir toda la información, teniendo en cuenta los distintos soportes o documentos donde esta pueda constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc. A tal efecto, una vez realizada la operación descrita, entregará una declaración por escrito al Departamento de Seguridad donde conste que así se ha realizado.