

## **PROYECTO FINAL DE INGENIERÍA**

# **DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE MIGRACIÓN DE PERSONAS**

**STEINFELD, Adalberto – LU92910**  
Ingeniería **Informática**

Tutor:  
**Mosettig, Octavio, NEC**

**21 de Agosto de 2015**



**UNIVERSIDAD ARGENTINA DE LA EMPRESA**  
**FACULTAD DE INGENIERÍA Y CIENCIAS EXACTAS**

**INDICE DE CONTENIDOS:**

<i>Índice de Contenidos:</i> .....	2
<b>AGRADECIMIENTOS</b> .....	<b>5</b>
<b>RESUMEN:</b> .....	<b>6</b>
<b>ABSTRACT:</b> .....	<b>9</b>
<b>CAPITULO 1</b> .....	<b>12</b>
OBJETIVO DEL PROYECTO.....	12
<i>Objetivos Específicos:</i> .....	12
ALCANCE DEL PLAN .....	12
<i>Supuestos y restricciones generales</i> .....	13
INTRODUCCIÓN .....	14
RESEÑA.....	14
ANTECEDENTES .....	16
CASOS DE ÉXITO DE LA BIOMETRÍA .....	18
GOBIERNO ELECTRÓNICO .....	23
<i>Las Estrategias de Gobierno Electrónico</i> .....	26
<i>Funciones de una estrategia de gobierno electrónico</i> .....	28
<b>CAPITULO 2</b> .....	<b>29</b>
ASPECTOS GENERALES SOBRE EL CONTROL MIGRATORIO .....	29
<i>¿Qué es el «control migratorio»?</i> .....	29
<i>¿Dónde puede llevar a cabo un Estado sus funciones de control migratorio?</i> .....	30
<i>¿Cuáles son los conceptos centrales que sustentan el control migratorio?</i> .....	30
<i>¿Qué medidas han sido adoptadas por los Estados para controlar la movilidad humana?</i> .....	31
<i>¿Cuáles son las etapas del control migratorio?</i> .....	32
<i>¿Cuáles son los tipos de control migratorio que se ejecutan durante estas etapas?</i> .....	33
<i>¿Cómo se organizan las acciones de control migratorio?</i> .....	34
<i>Elementos del Control de Migración automatizado</i> .....	36
<i>Preguntas actuales sobre la biometría</i> .....	37
<i>Ventajas y desventajas de las distintas modalidades biométricas</i> .....	41
EL PROBLEMA.....	43
<b>CAPITULO 3</b> .....	<b>45</b>
PROCESO DE CONTROL DE MIGRACIÓN .....	45
LECTOR DE PASAPORTES ELEGIDO: REALPASS-V .....	48
<i>Características del RealPass-V</i> .....	49
<i>Conceptos teóricos en los cuales se respalda</i> .....	50
LECTOR DE HUELLAS DIGITALES ELEGIDO: REALSCAN-G10.....	53
<i>Características del algoritmo VeriFinger utilizado por RealScan-G10</i> .....	54
RECONOCIMIENTO DE ROSTRO E IRIS ELEGIDO: ICAM TD 100 .....	56
<i>Alta velocidad - Captura Dual Iris</i> .....	57
<i>Proceso de Captura de Imagen de Iris</i> .....	57
<i>Conceptos teóricos en los cuales se respalda</i> .....	59
RECONOCIMIENTO DE VENAS ELEJIDO: PALMSECURE .....	60
<i>Principales características:</i> .....	61
<i>Potencial</i> .....	63
<i>La palma versus el dedo</i> .....	64

<b>CAPITULO 4</b> .....	<b>66</b>
OBJETIVOS DEL PRODUCTO .....	66
<i>Descripción Funcional</i> .....	67
<i>Beneficios</i> .....	69
WORFLOW GENERAL DE LA INSPECCIÓN PRIMARIA.....	70
<i>Inspección Primaria</i> .....	71
<i>Inspección Secundaria</i> .....	75
ARQUITECTURA DEL SISTEMA INTEGRAL DE CONTROL MIGRATORIO.....	77
MODELO DE NEGOCIO .....	79
a) <i>Identificación de los estados</i> .....	79
b) <i>Identificación de los casos del negocio</i> .....	79
c) <i>Propuesta Funcional</i> .....	80
REQUERIMIENTO DE CONFIGURACIÓN: .....	81
ACTORES.....	81
CASOS DE USO.....	86
REQUERIMIENTO NO FUNCIONALES:.....	109
REQUERIMIENTOS FUNCIONALES .....	112
DISCUSIÓN .....	130
<b>CAPÍTULO 5</b> .....	<b>131</b>
PLAN DEL PROYECTO .....	131
<i>Descripción de los Productos y Servicios</i> .....	132
<i>Despliegue y Puesta en Marcha</i> .....	134
<i>Metodología de implementación</i> .....	135
<i>Entregables del Proyecto</i> .....	136
<i>Control de Cambios</i> .....	137
<i>Plan de Capacitación</i> .....	138
<i>Comunicaciones del Proyecto</i> .....	141
<i>Riesgos detectados</i> .....	142
<i>Administración de Riesgos</i> .....	144
<i>Hoja de Trabajo para el Análisis de Riesgo</i> .....	144
<b>CONCLUSIONES</b> .....	<b>147</b>
<b>BIBLIOGRAFÍA</b> .....	<b>149</b>
<b>ANEXO A</b> .....	<b>152</b>
DESCRIPCIÓN DE LOS COMPONENTES DACTILARES.....	152
<i>Resultados de las Pruebas de Confiabilidad y Desempeño</i> .....	156
<b>ANEXO B</b> .....	<b>158</b>
DESCRIPCIÓN DE LOS COMPONENTES DE IDENTIFICACIÓN DE IRIS PARA SOLUCIONES STAND-ALONE WEB .....	158
<i>Descripción de Verieyes</i> .....	158
<i>Ventajas de VeriEyes</i> .....	158
<i>Capacidades y Características del Algoritmo VeriEyes</i> .....	159
DESCRIPCIONES DE COMPONENTES BIOMÉTRICOS .....	160
<i>Resultados de las pruebas de confiabilidad</i> .....	162
<b>ANEXO C</b> .....	<b>164</b>
IDENTIFICACIÓN DE ROSTROS PARA SISTEMAS STAND-ALONE Y APLICACIONES PARA AMBIENTE WEB.....	164
<i>Identificación Facial</i> .....	164
<i>Tecnología de Reconocimiento facial</i> .....	165
<i>Capacidades y Características del algoritmo VeriLook</i> .....	166
<i>Contenido de VeriLook 5.6 Standard SDK y Extended SDK</i> .....	167
DESCRIPCIÓN DE LOS COMPONENTES BIOMÉTRICOS.....	168

---

RECOMENDACIONES BÁSICAS PARA IDENTIFICACIÓN DE ROSTROS .....	169
PRUEBAS DE CONFIABILIDAD Y RENDIMIENTO .....	173
<b>ANEXO D .....</b>	<b>175</b>
IDENTIFICACIÓN AFIS Y MULTIBIOMÉTRICA PARA PROYECTOS DE GRAN ESCALA .....	175
<i>Descripción de MegaMatcher</i> .....	175
<i>Ventajas de MegaMatcher</i> .....	175
UTILIZADOS DE SISTEMAS BIOMÉTRICOS DE GRAN ESCALA.....	176
CAPACIDADES Y CARACTERÍSTICAS DEL ALGORITMO MEGAMATCHER.....	178
DESCRIPCIÓN DE LOS COMPONENTES DE SERVER Y CLÚSTER.....	183
<b>ANEXO E.....</b>	<b>186</b>
DESCRIPCIÓN DE COMPONENTES DE LA PALMA DE LA MANO.....	186
<i>Seguridad siempre a mano</i> .....	187
<i>Funciones y destacados</i> .....	190
<b>ANEXO F.....</b>	<b>193</b>
TRADUCCIÓN DEL MANUAL SDK DEL REALPASS-F VERSIÓN 1.0.....	193
<i>Función Básica</i> .....	193
<i>Usabilidad</i> .....	197
<i>Procedimientos de lectura de documentos</i> .....	198

## **Agradecimientos**

A la Universidad, por brindar esta oportunidad, luego de casi 10 años de no saber cómo plantear una propuesta, la simple oportunidad de una nueva entrega me generó la necesidad de aprovecharla.

A mi Padre y mi familia que me apoyó a lo largo de toda la carrera y nunca dejaron de creer que yo era capaz.

A mi Tutor que me brindó el apoyo necesario para concretar ideas generales y poder transformarlas en ideas prácticas, acompañándome en el periodo de desarrollo con recomendaciones certeras y concretas.

Y a mi Pareja por soportar las ansiedades y noches de poco sueño por ésta.

## Resumen:

El proyecto tiene como objetivo diseñar un sistema de control migratorio Clase A (máximo nivel para esta clase de sistemas de control, según los parámetros más exigentes de EEUU para no requerir Visa en el movimiento migratorio) efectuando el control fronterizo en un país con flujo migratorio promedio, mediante puestos equipados con última tecnología en captura biométrica para identificar inequívocamente a cada pasajero y complementar la operación con la captura y control automática de los documentos de viaje.

La elección del marco teórico para la aplicación del sistema de migración de personas sobre los conceptos de e-governance, se basa en la necesidad de dar cuenta de una serie de eventos (como cambio de paradigma, sociedad del conocimiento e innovación en las organizaciones públicas, entre otros) que han sido conceptualizados ampliamente por diversos autores.

Debe ser tomado como un complemento en políticas de e-governance y permitir al gobierno que lo implemente considerar información oportuna y precisa respecto al movimiento migratorio, contribuyendo a efectuar acciones que promuevan la participación, la transparencia y la colaboración, promoviendo un gobierno más eficiente y eficaz facilitando la gestión de los servicios del gobierno.

La cuestión es cómo llevar a cabo esta tarea de control de migración, teniendo en cuenta los actuales avances en la tecnología biométrica y su reciente implementación para dichos controles. Luego del análisis de las diferentes características biométricas que se pueden utilizar para identificar a un individuo, el avance de los dispositivos de lectura para evitar falsas identificaciones, y su implementación en diferentes controles, procediendo a analizar los actuales controles biométricos para el control migratorio en el mercado (detección de huellas y rostros) y para complementar la verificación automatizada de la documentación con dispositivos avanzados de verificación automatizada.

El uso de las tecnologías de la información y de las comunicaciones aplicadas en este proyecto permiten al gobierno ser más eficaz y eficiente al momento de identificar a los pasajeros y constituye una nueva manera de mirar las relaciones entre las tecnologías de la información y la gestión pública, promoviendo medios ágiles de información y comunicación para los ciudadanos y sus representantes.

En este caso, se seleccionó el lector RealPass-V, que no sólo registra la documentación de viaje, sino que también verifica la autenticidad y cruza los datos electrónicos con los datos visuales de una manera rápida y sencilla. Complementando el control de la información biométrica con la Lectura de Rostro e Iris en un mismo dispositivo (en este caso se seleccionó el lector iCAM TD 100) habilitamos a efectuar no sólo el control del Rostro y a cruzarlo con los datos de organismos internos y externos, sino también a profundizar en una segunda instancia realizando la lectura del Iris, lo que permite un control más exhaustivo del individuo sin invadir su integridad personal innecesariamente.

Finalizando los controles con la Lectura de Huellas Dactilares hecha por uno de los mejores dispositivos del mercado (en este caso, el RealScan-G10 de Suprema) y completar esa acción con la lectura de las venas de la mano (a través del dispositivo PalmSecure de Fujitsu) convierte al sistema descrito en uno de gran precisión dado que, aun cuando las huellas dactilares pueden ser alteradas por factores externos, el mapa de las venas prácticamente no cambia.

En el diseño de este sistema de control migratorio, no sólo deben ser contemplados el registro del pasajero y el control de su documentación y/o datos biométricos, sino que también deben considerarse el control de listas negras provista por organismos externos o internos (por ejemplo: Interpol, FBI, Juzgados, etc.), las reglas para menores, el control de Visa y los días de permanencia, la mínima cantidad de tiempo que el pasajero dispondrá para realizar su registro y la posibilidad de diseñar nuevas reglas, de acuerdo con el gobierno que lo implemente, para efectuar controles más exhaustivos en el futuro.

Si por cualquier motivo el pasajero no superara los controles en el tiempo estipulado para tal fin, deberá ser derivado a una inspección secundaria a realizarse por un Supervisor que efectuará los correspondientes controles manuales complementarios, habilitar o rechazar el movimiento migratorio y dejar registrada la decisión en una Base de Datos con información digitalizada (demográfica y multibiométrica) avalada por firma electrónica, permitiendo así respaldarla ante eventuales consultas legales, evitando que el soporte físico papel ocupe un lugar innecesario y evitando el consumo de recursos escasos.

Se dispondrá así de un nuevo sistema de control migratorio de última tecnología que, cumpliendo con los estándares ICAO (International Civil Aviation Organization), permita la verificación de autenticidad de la documentación presentada por el viajero (pasaporte y/o documento de viaje) y la agilización de los tiempos de atención en los puestos fronterizos mediante la automatización en los procesos de registración.

Facilitando que los niveles de dirección obtengan estadísticas para verificar el flujo migratorio y la distribución del mismo por seccional y tipo de transporte, de esa manera permitirá la concreción de mejoras en los servicios públicos que se brindan a la comunidad.



## **Abstract:**

This project aims to design a system of migration control Class A (the highest level for this kind of control systems, according to the most demanding parameters not to require Visa for the migratory movement) carrying out border control in a country with flow average migration through last posts equipped with biometric capture technology to uniquely identify each passenger and complement the capture operation and automatic control of travel documents.

The choice of the theoretical framework for implementing the system of migration of people to the concepts of e-government is based on the need to account for a series of events (as a paradigm shift, knowledge society, and innovation in public organizations, among others) that they have been conceptualized.

It should be taken as a complement to e-governance policies and it should allow the government that implements it to consider timely and accurate information regarding the migratory movement, helping to carry out actions to encourage participation, transparency and collaboration, promoting a more efficient government and facilitating effective management of government services.

The question is how to accomplish this task of controlling migration taking into account the current developments in biometric technology and its recent implementation in those controls. After analyzing the various biometric features that can be used to identify an individual, the advance on reading devices to prevent false identifications, and its implementation in different controls, we proceed to analyzed existing biometric controls to control migration on the market (to detect, for instance, fingerprints and faces) and to complement the automated verification of documentation with advanced devices for automated verification of such documentation.

The use of information and communication technologies applied in this project allows the government to be more effective and efficient when identifying passengers and represents a new way of looking at the relationship between information technology and governance, promoting agile media and communication for citizens and their representatives.

In this case, we selected the reader RealPass-V, which not only records the travel documents, but also verifies the authenticity of electronic data and intersects it with the visual data in a quickly and easy way. Complementing the biometric information control with Face and Iris Reading in only one device (in this case, we selected the iCAM TD 100 reader) we enabled to make not only the Face control, and to cross it with internal and external agencies' data, but to delve into a second instance by making Iris reading as well, allowing a more exhaustive control of the individual without invading the person unnecessarily.

Ending controls with Fingerprint Reading made by one of the best devices on the market (in this case, the RealScan-G10 of Suprema) and completing that with hand veins reading (via the Fujitsu PalmSecure device) the described system becomes accurate because, even if fingerprints can be affected by external factors, the map of the veins remains practically unchanged.

In the designing of this system of migration control not only we should take into account the registration and control of the passenger documentation and/or his biometric data, but we also should consider controlling blacklists provided by external or internal bodies (eg: Interpol, FBI, courts, etc.), the rules for kids underage, the control of Visa and the days of stay, the minimum amount of time that the passenger have to make registration and the possibility of designing new rules, according to the government that implements it, to make more thorough checks in the future.

If, for any reason, the passenger does not exceed controls in the stipulated time for this purpose, he shall be referred to a secondary inspection performed by a Supervisor who should make the corresponding manual controls, enable or reject the migration and keep records of the decision in a database with digitized information (demographic and multi-biometric) supported by electronic signature, allowing its support against possible legal consultations, preventing the paper hardware occupy unnecessary space and avoiding the consumption of scarce resources.

There will be a new system of migration control of latest technology, complying with ICAO standards (International Civil Aviation Organization), that allows verifying the authenticity of the passenger's documentation (passport and/or travel document) and streamlining service times at border posts by automating the registration processes.

Facilitating to management levels obtaining statistics to verify the immigration flow and its distribution by branch and type of transport; in this way this new system will enable to improve the public services provided to the community.

## CAPITULO 1

### OBJETIVO DEL PROYECTO

*Diseñar un sistema de control migratorio de personas Clase A (Máximo nivel para estos sistemas) integrando varios periféricos biométricos de vanguardia.*

#### **OBJETIVOS ESPECÍFICOS:**

- Identificar el aporte, de mejores prácticas de gobierno electrónico, al registro de movimientos migratorios de personas y la colaboración de diferentes controles externos.
- Efectuar un relevamiento de información en lo referente a registros biométricos de personas mediante diferentes periféricos, contemplando los últimos avances en esta tecnología.
- Analizar el diseño de un sistema informático que permita mejorar los procesos automatizados de control de personas y su posterior derivación en caso de encontrar posibles alertas positivas a analizar, según normativas internacionales.

### ALCANCE DEL PLAN

Para la creación de este nuevo sistema se diseñará la integración de varios periféricos del uso de biometría entre ellos el sistema AFIS (Automated Fingerprint Identification System) para control biométrico de huellas, complementando con lector de vasos sanguíneos de estas, como el sistema NEO FACE para examen de rostros y posterior análisis de Iris de las personas, sumando a ello la última tecnología en pasaportes para la validación de documentos (Chip RFID) e infrarrojo, todos ellos nunca integrados en un sistema de control migratorio de personas.

La integración de todos estos periféricos permitirá la creación de un sistema con el que se podrá realizar la supervisión de ingresos y egresos a un país por vía terrestre, aérea y marítima. En el cual se controlará la información propia ya registrada, y se complementará con el módulo de Blacklist permitiendo la conexión con entidades de seguridad mundial como por ejemplo la INTERPOL.

**SUPUESTOS Y RESTRICCIONES GENERALES**

Se han considerado los siguientes supuestos:

- ✓ La plataforma de hardware sobre la que se instalará el producto será provista por una consultora a seleccionar por el Gobierno Nacional que implemente el control migratorio, de acuerdo a los lineamientos de configuración proporcionados por este proyecto.

**Plataforma IT Propuesta**

Equipamiento	Data Center Principal	Data Center Secundario	Repuestos
Server Intel® Xeon® E5-2600 v3 series 18-core processors - 64 GB Ram - RAID 2 x 250GB	12	12	4
Server Intel® Xeon® E5-2600 v3 series 18-core processors - 128 GB Ram - RAID 2 x 250GB + 2 FCH	2	2	2
Server Storage 20 TB Cifrado SAS HDD / NL SAS HDD	1	1	0

- ✓ La instalación de la solución estará a cargo de este proyecto
- ✓ No se contempla la provisión de hardware por parte del proyecto.
- ✓ No se contempla la instalación de la red de comunicaciones requerida por parte del proyecto.
- ✓ No se contempla la carga de contenidos iniciales ni migración de datos por parte del proyecto.

## INTRODUCCIÓN

Lo que presenta este trabajo se basa en el “control migratorio de personas” aportando información fundamental para la toma de decisiones a nivel nacional sobre su propia población y la extranjera, analizando los movimientos migratorios y cruzarlos con los movimientos de éstos en el territorio nacional.

Los conceptos de e-governance aportan de forma electrónica dicha información, y la posibilidad de compararla online durante el tiempo y con estadísticas, tanto de movimientos como de los actos de los extranjeros en territorio nacional.

Por lo cual considerar un sistema de control migratorio confiable que contemple control biométrico de avanzada, para la detección certera de personas, es fundamental para cualquier estado que desee implementar políticas sociales responsables.

## RESEÑA

Actualmente en Argentina, como a nivel mundial según la organización internacional para la migración, se asume que el control Biométrico mediante las huellas dactilares y la digitalización de su documento son insuficientes, por tal motivo se está estableciendo nuevos controles adicionales para identificar a las personas considerando reconocimiento de rostros e incorporando dicha información en los nuevos pasaportes ser comparados en el momento del movimiento migratorio.

Se está instalando en todos sus pasos fronterizos, comenzando por aeropuertos y terminales de la empresa BuqueBus, el Sistema Integral de Captura Migratoria (S.I.C.A.M.) que funcionará online en todo el territorio Argentino. El mismo consiste en la toma fotográfica y captura de la huella dactilar, ambas almacenadas en forma digital en una base de datos propia complementada con el escaneo del documento de viaje –que registra de modo electrónico los datos patronímicos- más el uso de firma digital del Inspector, que es quien valida el movimiento migratorio.

Las autoridades de Migración de Argentina firmaron con varios países latinoamericanos acuerdos de cooperación y asistencia técnica para la implementación de este sistema en estos países, lo cual hará de este sistema un referente en control migratorio.

La Unión Europea contempla un visado Biométrico (con captación y registro de los datos biométricos del solicitante de dicha Visa Schengen donde incluye las diez impresiones dactilares y una fotografía digital).

Dichos controles no difieren mucho del contemplado por la Argentina.

El sistema de información Schengen proporciona a los países Europeos participantes una “Lista de Alerta” de personas que han cometido delitos y no les es admitido su ingreso a los países miembros. La Lista de Alerta de migración es similar a la utilizada por Australia con un sistema electrónico de vigilancia o advertencia temprana que permite a las autoridades de inmigración verificar si hay un problema conocido que podría afectar el otorgamiento de una Visa válida. Los Estados Unidos mantienen un sistema automatizado de vigilancia y apoyo consular que contiene información sobre criminales y terroristas conocidos. De acuerdo con la ley, los funcionarios consulares deben verificar la base de datos antes de expedir una Visa. (1)

En los Estados Unidos se opera con un sistema de Servicio Acelerado de Pasajeros (INSPASS), bajo el cual los viajeros inscritos, después de la autorización a través del sistema de vigilancia, reciben una tarjeta codificada con información Biométrica de Identificación (usando geometría de la mano). Cuando el viajero llega a una cabina de INSPASS especialmente adecuada para el examen de dicha tarjeta y la lectura Biométrica de la mano, especialmente ubicadas en Aeropuertos, los datos biométricos previamente capturados establecen la identidad al ser cruzados con los que se capturan en el momento de la migración.

Por conclusión, la implementación del sistema aquí propuesto con periféricos Biométricos como lectores de huellas dactilares complementado con lector de vasos sanguíneos, y reconocimiento de rostro e iris más la lectura del RFDI de los nuevos pasaportes que contemplan la información digitalizada del rostro, y/o la verificación infrarroja del mismo, hacen que éste sistema se encuentre un paso más adelante que lo ofrecido hoy en el mercado en la identificación inequívoca de las personas y así poder efectuar un control más apropiado en los movimientos migratorios.

## **ANTECEDENTES**

En este contexto, los sistemas actuales de control de flujos migratorios, plantean desarrollos tecnológicos integrando capacidades de análisis sobre algunas dimensiones acotadas del problema, para tomar las decisiones de alto nivel requeridas y acciones preventivas de control. Así la Dirección Nacional de Migración Argentina (2) (que ejerce el poder de policía migratoria y decide sobre la admisión de personas en territorio nacional) fomenta la descentralización por lo cual la correlación entre diferentes sectores autónomos es fundamental.

Aún con la tecnología de reconocimiento facial cada vez más avanzada, hay un dilema ético que en este trabajo no se profundizará, contemplando su ejemplo en el caso de Inglaterra, quien fue uno de los pioneros en utilizar esta tecnología no solo para el control migratorio de personas, y que en el 2010 desmanteló su sistema nacional de identificación de personas debido al reclamo público por lo invasivo que esto resulta.

La Argentina desde 2011 ha avanzado mucho con la referencia cruzada entre el sistema de migración desarrollado y la información asimilada por el Registro Nacional de Personas (Renaper) donde el registro de información Biométrica ya no está limitado solo a sospechosos o convictos de delitos criminales.

El dilema ético es que dicha información no se limita solo a información biométrica, también registrar: estado civil, grupo sanguíneo, parentescos y otra información básica que describen más que rasgos físicos, también rasgos intelectuales, y de trasfondo culturales, que se vienen registrando desde el 2012 en los recién nacido según decreto 1051 del poder ejecutivo.

Conjuntamente con la información biométrica se podrá identificar no solo un rostro anónimo entre miles, con la creciente utilización de cámaras para el control de la seguridad por parte del estado (organismos de seguridad como Policía Federal, Gendarmería, Prefectura, Policías Provinciales o Municipales) y otros organismos estatales, quienes cruzando



información con datos biométrica y otros datos personales podrían violar principios esenciales de las sociedades libres al facilitar la localización y el seguimiento de personas, no solo de sospechosos o convictos de delitos criminales, centralizando peligrosamente estos datos, con el consiguiente riesgos de abuso por parte del estado como los ya sufridos.

Por ello, si simplemente citaremos un par de puntos que contempla el mal uso de la biometría por parte del estado:

- Da demasiado poder al estado a costa de libertades individuales.
- Viola el derecho a la privacidad y el principio de presunción de inocencia.
- Es un arma de doble filo por el potencial abuso de los datos almacenados.
- La biometría no es una tecnología infalible y ya se han demostrado muchos de sus fallos.
- La biometría es una tecnología que mientras más tolerada y aceptada sea, más facilita la implantación de un estado totalitario.

## CASOS DE ÉXITO DE LA BIOMETRÍA

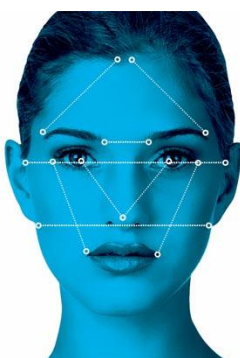
Un dato biométrico es una característica física única que permite identificar con poco margen de error a una persona. Ejemplo de estos datos son las huellas dactilares, el ADN, la geometría de la mano, análisis del iris, análisis de retina, venas del dorso de la mano, reconocimiento facial, patrón de voz, firma manuscrita, análisis gestual, etc.



El más reconocido de ellos es la huella dactilar, donde uno de los últimos avances de la tecnología en este campo es la datación de la misma (Investigación efectuada por parte del instituto médico-legal holandés (NFI) (3)) lo cual permite avanzar en la criminología, identificando el momento en el cual dicha huella fue plasmada situando al sospechoso en tiempo y lugar.

El Mekong Developmen Bank, un banco que opera en Vietnam, ha implementado una solución biométrica de reconocimiento dactilar que posibilita obtener dinero conjuntamente con la tarjeta de débito. Se espera que con esta nueva tarjeta que identifica a su titular inequívocamente, se amplíe el acceso a servicios bancarios para las poblaciones rurales y urbanas de Vietnam ya que en este país –que cuenta con una población de 86 millones de personas- sólo el 20% tiene una cuenta de banco.

(4) En Colombia implementaron un sistema para que las Loterías Nacionales registren las huellas digitales de quienes participan para identificar rápidamente a los clientes que compren los billetes y fracciones de lotería, y cuando ganan premios hacer la confrontación correspondiente y así evitar cualquier posible error de la concesión debido a equivocaciones.



Respecto al reconocimiento facial, el FBI está invirtiendo en mejorar el sistema de identificación biométrica mediante esta característica, que sumada al reconocimiento de ADN e incluso registro de voz constituirán el sistema NGI (Identificación de Próxima Generación – Next Generation Identification) y permitirá analizar 1,6 millones de fotos de pasaportes o de archivos e identificar una persona en 1,2 segundos y con una precisión del 92%. El NGI reemplazará al Sistema Integrado Automatizado de Identificación de Huellas Dactilares (IAFIS, por sus siglas en Inglés), lo que permitirá al FBI procesar de forma más rápida la información y compartirla con corporaciones locales, estatales, federales e internacionales. (5)

En la universidad Rey Juan Carlos de Madrid han probado con éxito un sistema de reconocimiento facial biométrico en 3D y responde muy bien ante distintas situaciones, siempre que la grabación sea de calidad. La particularidad de esta tecnología, frente a las utilizadas en otros aeropuertos del mundo, es que establece un gráfico con imágenes en 3D de los rostros sospechosos. Las imágenes deseadas se envían a la Policía Nacional y a la Guardia Civil para su comparación con el fondo de imágenes de los criminales. (6)

En la Red de Justicia de Pennsylvania, tanto estatales como federales utilizarán un nuevo programa de biometría facial para identificar sospechosos o testigos en base a las fotos y videos tomados por cámaras de vigilancia. El programa ForensicaGPS de Animetrics será incorporado al sistema de reconocimiento facial (JFRS) de JNET, logrando que este sea más ágil y preciso en las investigaciones policiales. (7)

ForensicaGPS, accionando por tecnología FACEngine de Animetrics, toma imágenes 2D de vigilancia por video o fotografías y las convierte a 3D mediante software de reconocimiento facial patentado por Animetrics. De esta imagen tridimensional, “se puede construir una imagen facial de identificación, lo que hace más fácil la confirmación de la identidad cuando se compara con casi tres millones de imágenes que se han acumulado desde 1998 en la base de datos de Pennsylvania”.

Facebook ha eliminado todos los informes de sus datos europeos de reconocimiento facial, a raíz de la presión de los organismos de protección de datos de irlandeses y alemanes el año pasado (2014). Facebook había utilizado el poder de la tecnología de reconocimiento facial para sugerir que los usuarios deben “marcar” en las fotos su identidad. El servicio fue desactivado en la UE en los últimos meses del año pasado y también fue suspendido en los EE.UU. Sin embargo, parece que los usuarios estadounidenses de la red social recibirán este servicio nuevamente. (8)



También encontramos estudios del IEEE (Instituto de Ingeniería Eléctricos y Electrónicos) que profundizan sobre el inconveniente que provoca falsas coincidencias ocasionadas por el envejecimiento del iris, y genera un modelo de lectura que incluye los cambios relacionados con la edad en la dilatación de la pupila.

Los investigadores analizaron los resultados de un conjunto de datos a intervalos de tres años, y descubrieron un aumento del 150% en la tasa de no-mach falsas en un umbral de decisión que representa una de cada dos millones de tasas de falsa coincidencia. El documento

resume varios elementos conocidos del envejecimiento del ojo que pueden contribuir en mejorar el modelo de lectura, incluyendo los cambios relacionados con la edad en la dilatación de la pupila. (9)

Un nuevo sistema biométrico de seguridad basado en el movimiento de los ojos está siendo desarrollado por técnicos en Finlandia. El equipo publicó una nota en la revista *International Journal of Biometrics* explicando cómo las sacadas (esos pequeños pero rápidos movimientos involuntarios de los ojos) pueden medirse con una cámara de video especial. De acuerdo al grupo de técnicos finlandeses, el patrón de movimientos sacádicos es tan único como una huella digital o el iris pero más fácil de grabar y por tanto, proveer una alternativa a la tecnología de identificación biométrica.

El equipo ha estudiado los movimientos oculares otoneurológicos durante varios años y concluyó que ciertos valores estadísticos que se pueden extraer de los datos para estos movimientos son únicos para cada uno de nosotros.



El reconocimiento de venas ha visto un incremento en su uso en todo el mundo en los últimos años. Hitachi, Ltd. cree que puede proveer de tecnología segura de firma digital basada en el patrón de las venas.

El trabajo presentado en el Simposio 30 en Criptografía y Seguridad de la Información (SCIS 2013) celebrado en Kyoto, Hitachi dice que su nueva tecnología será desarrollada como una tecnología que complemente la firma digital, práctica y segura, en aplicaciones para en los sistemas de identificación nacional, servicios de gobierno electrónico y el comercio electrónico.

El problema con el uso de datos biométricos, tales como patrón de las venas del dedo como “clave secreta” en una arquitectura de PKI, es que se trata de datos que pueden variar con las condiciones ambientales y la condición física de la persona, a lo que Hitachi replica que se puede producir una tecnología segura de firma digital basada en el uso de información biométrica, a pesar de estas variaciones. (10)

El fabricante de microprocesadores Intel Corporation, también trabaja sobre esta línea, pretendiendo superar el uso tradicional de las contraseñas reemplazándolas con comandos biométricos de reconocimiento de los patrones de las venas de las manos.

De acuerdo al portal de noticias por Internet Bloomberg, científicos de la compañía ventilaron a manera de demostración un sistema que tiene la capacidad de reconocer el patrón de venas de la mano de los usuarios que a través de un sensor especializado dichos datos de

reconocimiento biométrico son enviados automáticamente a la central de cómputos para sustituir el tradicional uso de los teclados para colocar las contraseñas de acceso a Internet.

Este demo fue presentado durante la celebración del Foro Anual para Desarrolladores que organizó Intel en la ciudad de San Francisco en agosto de 2012 y se mostró como una tecnología de evaluación a ser incorporada en las tabletas electrónicas y computadoras portátiles que incluyan arquitectura de procesamiento de la compañía.

Dentro de los controles no convencionales hoy en día existen sistemas para el control de acceso biométrico, los cuales pueden basarse en cualidades físicas o del comportamiento de las personas. Por el lado de las cualidades físicas, éstas están relacionadas con la forma del cuerpo. En este caso, se puede hablar de los chequeos de huellas digitales, del reconocimiento facial y el escaneo de la retina, entre otros.

Las cualidades de comportamiento incluyen cuestiones como el ritmo de tecleo, la forma de caminar y la voz. En el presente y en muchos lugares, es posible ver dispositivos para el reconocimiento de voz, los cuales, a pesar de lo que se pudiera pensar, aportan un alto rendimiento.



Verbio, multinacional fabricante de software de reconocimiento de voz (ASR) y síntesis de voz (TTS) ha desarrollado un sistema de síntesis de voz en portugués brasilero capaz de pronunciar correctamente una amplia variedad de nombres y apellidos existentes en Brasil.

Este sistema de síntesis de voz, disponible en Brasil desde el 2013, incluye por primera vez un innovador sistema que permite la inclusión de nombres y apellidos fonéticamente no propiamente portuguesa, cómo es el caso de nombres y apellidos japoneses, eslavos, alemanes, españoles, etc.

Durante los últimos años este sistema de locución y reconocimiento de vos de forma automática ha incrementado su presencia en los entornos telefónicos automáticos, denominados IVR o portal de voz, principalmente por la ventaja que ofrece a la hora de ofrecer al usuario información personalizada, pero también de una manera más ágil y económica a la empresa.

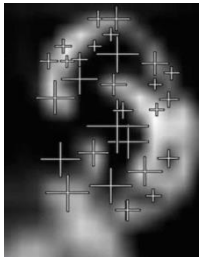


Investigadores chinos han encontrado una manera de mejorar el rendimiento de un sistema biométrico diseñado para reconocer a las personas basándose en el sonido de los latidos del corazón.

El trabajo presentado por los investigadores de la Universidad de Hangzhou Dienzi presenta un sonido cardíaco basado en el análisis del espectro marginal, que es una técnica de extracción de características para fines de identificación. Los resultados indican que la técnica aumenta la tasa de reconocimiento a 94,4% en comparación con el de las técnicas tradicionales (84,32%) fundamentalmente basado en una base de datos de 280 sonidos del corazón de 40 participantes.

Los ruidos cardíacos son un reflejo del movimiento mecánico del corazón y del sistema cardiovascular. La característica particular es que contiene información fisiológica y patológica sobre el corazón y varias partes del cuerpo.

Existen multitud de otros aspectos del cuerpo que podrían servir como identificadores inequívocos y en los que se está investigando su viabilidad.



Este podría ser el caso del reconocimiento según la forma de la oreja. Actualmente expertos de la Universidad de Leicester (Inglaterra) están desarrollando esta tecnología que se basa en la toma de fotografías de este órgano para su posterior análisis a través de software y contrastación con una base de datos existente.

La ventaja de este sistema es que es resulta menos agresivo que otros como el escáner de retina o la huella digital al no existir un contacto físico. Igualmente en el estudio se investiga cual es la distancia máxima a la que podría tomarse la fotografía para realizar una identificación fiable.

En la imagen, puede observarse una instantánea de una oreja y la definición, por parte de un software, de sus trazas más importantes que serán contrastadas. La gran desventaja de este sistema es la facilidad, dado los avances en maquillaje y cirugía plástica, de engaño al sistema mediante elementos postizos pues, como se ha comentado, sólo se analiza la forma de la oreja y ningún otro parámetro.

Entre las técnicas con márgenes de error aún amplios pese a que se está logrando grandes avances estarían las de reconocimiento de la forma de caminar, de teclear en el ordenador o la identificación por el olor corporal discriminando aromas como el sudor.

---

## GOBIERNO ELECTRÓNICO

El gobierno electrónico está enmarcado dentro del gobierno abierto, y es una herramienta que ayuda los gobiernos a efectuar acciones que promueven la participación, la transparencia y la colaboración, promoviendo un gobierno más eficiente y eficaz para facilitar la gestión de los servicios del gobierno y hacerlo más accesibles permitiendo un mayor acceso público a la información, y para hacer al gobierno mayor responsable ante los ciudadanos.

Los países desarrollados están resolviendo buena parte de los problemas de funcionamiento de sus gobiernos mediante la incorporación masiva de las nuevas tecnologías de la información y comunicación, para mejorar los procesos internos de toma de decisiones y para mejorar la relación con la ciudadanía. (11)

El uso de las tecnologías de la información y comunicación permite que el gobierno torna más eficaz y eficiente, proporciona servicios de más calidad y fácil acceso, estimula la actividad económica, sirve como apoyo en la difusión de programas y rendición de cuentas, sirve como guía de autogestión al ciudadano, incrementa la comunicación tanto al interior como al exterior del gobierno, genera certidumbre y confianza en el gobierno, informa a la población y crea un ambiente que facilita la participación. (12)

En concreto, el Gobierno Electrónico se refiere al uso por parte de las agencias gubernamentales de las Tecnologías, que tienen la capacidad de transformar las relaciones con el ciudadano, las empresas y diversas dependencias gubernamentales, englobando por lo menos los siguientes elementos:

- Está relacionado con la aplicación de las Tecnologías.
- Implica innovación en las relaciones internas y externas del gobierno (ya sea con otros organismos gubernamentales, sus propios empleados, las empresas y/o el ciudadano.
- Afectar la organización y función de gobierno en lo relativo a: Acceso a la información; Prestación de servicios; Realización de trámites; o Participación ciudadana.
- Busca optimizar el uso de los recursos para el logro de los objetivos de gobierno.
- Su implementación implica el paso por una serie de estados, no necesariamente consecutivos.
- Es un medio, no un fin en sí mismo.



El gobierno electrónico persigue incrementar la transparencia y eficiencia del sector público, proveer medios ágiles de información y comunicación para los ciudadanos. Asegurando el desarrollo sostenible. (13)

El gobierno electrónico constituye una nueva manera de mirar la relación entre tecnologías de información, gestión pública y acción política en un periodo histórico donde el cambio paradigmático atraviesa transversalmente todas las dimensiones del sistema mundial y las tecnologías de la información facilitan el proceso a partir de la creación de vínculos entre aquellos que poseen la información y quienes la requieren.

Específicamente el uso masivo de las tecnologías de la información y la comunicación en el ámbito de la administración pública ha motivado el interés general por encontrar mecanismos para que el gobierno electrónico impacte positivamente en la facilitación del traspaso de comunicación y tramitación de servicios por medios electrónicos. (14)

La búsqueda de un impacto positivo está asociada a la posibilidad de abrir canales de vinculación cada día más directos para acercar la gestión política a la ciudadanía, para promover la participación, responder a las demandas ciudadanas de mayor transparencia, y abordar con mayor eficacia la utilización de tiempos y recursos para realizar las transacciones.

Una cuestión de importancia a tener presente es que si bien la implantación del gobierno electrónico puede traer grandes beneficios, también puede generar mucha frustración si no se ponen en práctica las condiciones de éxito para este tipo de proyectos.

La elección del marco teórico para la aplicación del sistema de migración de personas sobre los conceptos de gobierno electrónico se basa en la necesidad de dar cuenta de una serie de eventos (como cambio de paradigma, sociedad del conocimiento, e innovación en las organizaciones públicas, entre otros) que han sido conceptualizados. (15)

La gestión del conocimiento se encuentra estrechamente relacionada con la recopilación, utilización y difusión de conocimiento mediante una infraestructura técnica y comunicacional, que tiene como objetivo la efectividad de nuestras interacciones.

“La gestión del conocimiento es la actividad organizacional de creación del entorno social e infraestructura para que, ese conocimiento, pueda ser accedido, compartido y creado.”

“La esencia del gerenciamiento consiste en hacer que el conocimiento sea más productivo. El gerenciamiento, en otras palabras es una función social. (16)



La cuestión es cómo llevar a cabo esta tarea de control de migración teniendo en cuenta que el conocimiento es algo más amplio y profundo que los datos y la información, dado que en su construcción entran en juego las capacidades de decodificación de la información e internalización individuales:

“El conocimiento debe distinguirse de la información: Poseer conocimientos, sea en la esfera que sea, es ser capaz de realizar actividades intelectuales o manuales. El conocimiento es por tanto capacidad cognoscitiva. La información en cambio es un conjunto de datos, estructurados y formateados pero inertes e interactivos hasta que no sean utilizados por quien tiene suficiente capacidad para interpretarlos y manipularlos”. (17)

Tal el motivo por el cual en el control migratorio no basta identificar a la persona inequívocamente. También debe considerarse todo su historial migratorio, como contemplar las posibles alertas de organismos externos como el FBI o la Comisión de Seguridad Europea.

La presión sobre los organismos públicos para mejorar sus servicios, para aumentar su eficiencia, para mostrar una mayor transparencia y entregar accesibilidad son cada vez mayores y en ese marco, las nuevas tecnologías de la información juegan un rol fundamental.

“Esas tecnologías de información son las herramientas que están produciendo los cambios más radicales en la gestión pública o privada, y paradójicamente, son las que más escapan a la comprensión o formación de la gran mayoría de los reformadores que están gestionando o financiando grandes proyectos de informatización pública” (18).

Los grandes proyectos tecnológicos enfrentan en todo el mundo enormes dificultades, con altas tasas de fracaso total o parcial, resistencias al cambio, y carencia de dirección estratégica por parte de las autoridades superiores, que suelen creer que éste es un problema para el jefe del departamento de informática. Es difícil que los ejecutivos públicos con visión de estrategia tecnológica provengan de las filas de los profesionales informáticos. (19)

La utilización de recursos de Tecnológicos para potenciar la capacidad de un gobierno en el logro de sus metas y entrega eficiente de sus servicios a los ciudadanos es absolutamente imprescindible. Con un Gobierno Electrónico la filosofía de las aplicaciones verticales cambia. Ya no hay aplicaciones aisladas, ahora son servicios que pueden usar y reutilizar, según su necesidad, los diversos departamentos y áreas de la organización compartiéndola con otras instituciones públicas.

Las consecuencias e impactos en la atención a los ciudadanos se expresan en al menos los siguientes aspectos: los usuarios pueden recibir atención sin restricción horaria y no importando en qué lugar geográfico se encuentren, los usuarios tienen acceso a información pública en forma simple, oportuna, clara y transparente; los usuarios pueden resolver sus problemas a través de un contacto único con el Estado, aunque se trate de requerimientos que involucren a más de una institución; los usuarios no están obligados a presentar ningún documento o certificar información que se encuentre disponible en formato electrónico por alguna institución pública, los usuarios pueden hacer transacciones financieras en forma electrónica, (por ejemplo pagar un certificado de nacimiento, o recibir el pago por un servicio prestado un organismo público si se es un proveedor del Estado).

Los ciudadanos son libres para consultar sobre información de los actos públicos del Estado que sea de su interés conocer. El Estado transparentará dichos actos dejándolos disponibles electrónicamente. Los ciudadanos tienen derecho a participar y expresar su opinión por medios electrónicos (e-participation).

La transacción en línea es más común en compras públicas, pago de impuestos, servicios de seguridad social, prestaciones del registro civil, aduana y migración, entre otros. La digitalización de los procesos administrativos aumenta su eficacia, brindando un servicio eficiente y amable a los ciudadanos, y puede contribuir a una mayor transparencia. El registro digital de la información de estos procesos puede ser un mecanismo para combatir el desperdicio de recursos y la corrupción. Utilizar Internet para que los ciudadanos accedan a servicios de salud, educación o a la realización de trámites, favorecerá una más rápida adopción de estas tecnologías en los hogares y las empresas. (20)

### **LAS ESTRATEGIAS DE GOBIERNO ELECTRÓNICO**

A pesar de la relativa juventud del término gobierno electrónico o e-governance, en los últimos 3 años han proliferado los documentos denominados estrategias de gobierno electrónico o planes de gobierno electrónico que, a la par que ordenan las acciones de los gobiernos que los diseñan, contribuyen a la consolidación del concepto e-governance. (21)

Si bien la aplicación de las tecnologías de la información al funcionamiento de la administración pública es casi tan vieja como la historia de la computadora, la combinación

de estas tecnologías con las tecnologías relacionadas de telecomunicación con una visión renovadora del gobierno y su forma de relacionarse con los ciudadanos, es mucho más reciente. La generalización del término gobierno electrónico para referirse a lo descrito en la frase anterior, el establecimiento de departamentos de e-governance en las empresas de consultoría y de tecnología, así como la intensificación de la realización de estudios, rankings y ensayos sobre el e-governance es un fenómeno de los últimos 5 años.

En cualquier caso, desde que en la primera mitad de los 90 internet cobra vida de forma parecida a como lo conocemos hoy, no en sus orígenes como ARPANET hace más de 30 años cuando Larry Roberts y su equipo buscaban un mecanismo seguro de comunicación ante un ataque a los mecanismos de comunicación tradicionales, los esfuerzos aislados por utilizarlo en la administración pública se han sucedido y algunos han quedado para la historia como pioneros del e-governance. (21)

Como ya se ha mencionado, es justo reconocer en este punto, la valiosa contribución en este aspecto de David Osborne y Ted Gaebler con su libro *Reinventing Government*, el cual se convirtió en fuente de inspiración para funcionarios públicos de todo el mundo durante la década de los 90, aludiendo a las tecnologías de la información y la comunicación como la excusa que los gobiernos necesitaban para cambiar y que los medios de comunicación precisaban para sentir cierta atracción por esta transformación.

Inspirados por éste libro y otros documentos acerca de las posibilidades de las “tecnologías de la información y la comunicación” como herramienta de transformación de la administración pública, algunos gobiernos, para ser precisos, algunas agencias o departamentos dentro de los gobiernos, se lanzan a experimentar con la posibilidad de empezar a manejar sus relaciones con los ciudadanos a través de internet.

En general, se trataba de esfuerzos aislados, dentro de agencias que tenían la fortuna de contar con algún recurso financiero extra para experimentar con las posibilidades del e-governance y, sobre todo, que contaban que con un líder dispuesto a asumir ciertos riesgos y manejar todas las dificultades de este tipo de procesos.

---

**FUNCIONES DE UNA ESTRATEGIA DE GOBIERNO ELECTRÓNICO**

A pesar de que como se ha comentado, algunos gobiernos como el de Estados Unidos, Brasil, Chile o Canadá llevan varios años produciendo iniciativas de gobierno electrónico y son internacionalmente reconocidos como países avanzados en esta área, y en su gran mayoría de estos países han desarrollado estrategias o planes de gobierno electrónico de forma relativamente reciente. En muchos casos, existían documentos o estudios relacionados con la incorporación de las tecnologías de información y comunicación al desarrollo del país en su conjunto, pero un documento enfocado en gobierno electrónico que contemple la gran mayoría de los aspectos mencionados en el apartado anterior, no se creó en gran parte de estos países hasta principios de esta década (21).

Un plan de gobierno electrónico cumple un rol que va más allá del aspecto coordinador y racionalizador del gasto público. Las principales contribuciones de un plan de gobierno electrónico podrían resumirse en los siguientes puntos:

- Mapa-guía para el avance del e-governance, que orienta las actuaciones de todos los implicados.
- Mecanismo de control, que permita asignar responsabilidades y monitorear el cumplimiento de las mismas.
- Elemento de referencia para la resolución de dudas operativas relacionadas con la implementación del e-governance.
- Instrumento de organización y manejo del cambio cultural necesario.
- Herramienta de marketing para la venta política del concepto que, bien utilizado, permite conseguir el indispensable apoyo político.
- Mecanismo de captación de recursos financieros que puede servir de referente para el establecimiento de alianzas con el sector privado, para la incorporación de inversores privados a proyectos de gobierno electrónico y para la asignación de los recursos públicos a aquellos proyectos que aporten mayor valor añadido al país.

El gobierno electrónico se observa como un medio para que los gobiernos modernicen sus procesos, mejoren sus interacciones con los ciudadanos y disminuyan la fractura digital existente entre estos. “Para los países en desarrollo, el gobierno electrónico es una gran oportunidad para mejorar la calidad y la eficiencia de la administración y la economía”. El hecho de que el gobierno electrónico no pueda tratarse en forma aislada o paralela del gobierno, lleva a los países a reevaluar la forma en que miden los beneficios del mismo, los objetivos propuestos y el concepto de gobierno electrónico en sí. (22)

---

## CAPITULO 2

### ASPECTOS GENERALES SOBRE EL CONTROL MIGRATORIO

#### *¿QUÉ ES EL «CONTROL MIGRATORIO»?*

El control migratorio es un concepto variado y poco concreto. Una prueba de esta situación son las diferentes conceptualizaciones en la legislación latinoamericana que relacionan el control migratorio con una serie de funciones que el Estado asume en relación con la traslación de las personas, sean nacionales o extranjeras. Estas diversas legislaciones discrepan en sus alcances generales y específicos, y evidencian esa falta de acuerdo en su conceptualización. (23)

El término hace referencia a la capacidad del Estado de verificar, vigilar, supervisar o autorizar la entrada, permanencia y salida de nacionales o extranjeros de un Estado, y de regular las consecuencias de su traslado. Para ello, establecen reglas de funcionamiento, organización y coordinación de los servicios vinculados con esta potestad estatal. Se pueden identificar, al menos, cuatro elementos que estructuran el concepto de control migratorio:

1) El cruce de una frontera entre dos Estados: entrada, salida o permanencia de personas, con diversos motivos, objetivos, plazos, entre otros elementos.

2) El ejercicio del poder estatal a través de acciones de verificación, vigilancia, supervisión o autorización en el marco de determinadas garantías para las personas en movimiento.

3) Una regulación por parte de un Estado (regímenes de movimiento, sistemas de control, entre otros), que las personas en movimiento deben respetar y cumplir.

4) Atribuciones, derechos y responsabilidades diferenciadas para los Estados y las personas, dependiendo del movimiento que realizan (entrar, salir o permanecer en un territorio) y la regulación que se establezca.

### ***¿DÓNDE PUEDE LLEVAR A CABO UN ESTADO SUS FUNCIONES DE CONTROL MIGRATORIO?***

Los Estados desarrollan sus funciones de control migratorio en los siguientes lugares (23):

- Dentro de su territorio
- En sus fronteras lineales
- En las zonas internacionales
- En terceros Estados, a través de sus funcionarios consulares, migratorios o policiales.

### ***¿CUÁLES SON LOS CONCEPTOS CENTRALES QUE SUSTENTAN EL CONTROL MIGRATORIO?***

Las justificaciones para la existencia de un control migratorio o de la movilidad humana se sustentan principalmente en dos conceptos (23):

- La soberanía de los Estados. Esta es la facultad de cada Estado de ejercer el poder sobre sí mismo y determinar las reglas que regirán su sistema de gobierno, su territorio y su población. En materia migratoria, y desde la perspectiva tradicional, implica la potestad estatal de decidir quién entra y quién sale de su territorio, y la manera en que lo hace.
- La seguridad nacional. Tradicionalmente, este concepto hace referencia a la potestad del Estado de proteger su territorio y a su población, e involucraba el uso legítimo de la fuerza, en manos del ejército y la policía. Así, se salvaguardaba la existencia misma del Estado, se defendía la delimitación territorial y se garantizaba la seguridad cotidiana de los nacionales.

**¿QUÉ MEDIDAS HAN SIDO ADOPTADAS POR LOS ESTADOS PARA CONTROLAR LA MOVILIDAD HUMANA?**

Bajo el enfoque de control restrictivo, las principales medidas adoptadas para controlar la movilidad humana internacional son las siguientes (23):

<p>Nuevos sistemas de identificación e información</p>	<p>La tecnología, generalmente, facilita los procesos de control migratorio. Hoy en día, muchos Estados han implementado una serie de medidas vinculadas con el uso de la biométrica, como el reconocimiento facial, la reproducción de huellas digitales y la geometría de manos. Por otro lado, la tecnificación en la emisión, y en los mecanismos de control de los documentos de identidad y de los documentos de viaje son mecanismos importantes que los Estados están implementando para mejorar el control migratorio. Entre las debilidades que los expertos atribuyen a la aplicación de estos mecanismos encontramos las siguientes:</p> <ul style="list-style-type: none"> <li>• Problemas relativos a la estandarización de los documentos e información, y la generalización en su uso</li> <li>• Alto costo de la infraestructura y tecnología que estos mecanismos requieren, por ejemplo, en términos de levantamiento y alimentación de datos</li> <li>• La multiplicidad de sistemas que utilizan los países, lo que dificulta los procesos de adaptación de los diferentes sistemas.</li> </ul>
<p>Aumento de las restricciones y los controles a la entrada de personas</p>	<p>Con respecto a las restricciones al ingreso, se evidencia, por un lado, el endurecimiento de los requisitos administrativos, como los relacionados con la solicitud de visas o autorización de ingreso a un territorio. Muchas veces, estos están determinados en función de características particulares de los grupos de personas que los Estados desean o rechazan que ingresen. Por otro lado, también existen medidas que buscan endurecer el control mediante el incremento de la presencia física del Estado, especialmente en las fronteras terrestres, como, por ejemplo, la asignación de un mayor número de personal de seguridad en los puestos de control (patrullas fronterizas) o el levantamiento de muros divisorios, entre otras medidas de este tipo.</p>
<p>Refuerzo de los controles migratorios a través de su «desterritorialización»</p>	<p>Actualmente, el control migratorio es aplicado más allá de las fronteras físicas de los Estados. El ejercicio de este control, en algunos casos, ha sobrepasado el propio ámbito de jurisdicción estatal. Por ejemplo, se verifica que empresas privadas, como las aerolíneas, se preocupan por ejercer un control documentario migratorio de manera anticipada e, inclusive, realizan inspecciones. Este control es ejercido debido a posibles sanciones o cargas que deban afrontar al transportar personas sin la documentación requerida.</p> <p>La “desterritorialización» del control ha llevado también al establecimiento de centros de retención preventivos en los países de origen y tránsito, así como el nombramiento de autoridades</p>

	migratorias de los países de destino para ejercer sus funciones en los países de origen.
Incremento de los controles internos	<p>La tendencia demuestra que la realización de «redadas» (operaciones a cargo de agentes especializados en migraciones que tienen como finalidad detectar infracciones a la normativa migratoria) es una práctica que va en incremento en las políticas migratorias actuales. Otras estrategias son las siguientes:</p> <ul style="list-style-type: none"> <li>• Introducir el conocimiento de la lengua nativa como determinante para acceder a la nacionalidad, y a los sistemas de atención y orientación.</li> <li>• Establecer restricciones a personas en movilidad referidas a la posibilidad de rentar viviendas, obtener permisos de conducir y acceder a los servicios sociales básicos.</li> <li>• Imponer multas a los empleadores y a aquellos que renten viviendas a personas en condición administrativa irregular.</li> </ul>
Fortalecimiento de la cooperación interestatal	<p>Las nuevas estrategias en relación con el control migratorio incluyen intervenciones articuladas entre las autoridades de países receptores, de tránsito y de origen. Por ejemplo, las acciones de INTERPOOL y de EUROPOOL buscan que los Estados miembros estén dotados de información en materia de crimen organizado. Por otro lado, los «acuerdos de readmisión» buscan facilitar el reingreso a sus países de origen a las personas que permanecen irregularmente en un Estado. Por lo general, estas medidas buscan «agilizar» la expulsión de los nacionales de terceros países, donde los Estados signatarios deben readmitir en su territorio, sin ninguna formalidad previa, a toda persona que posea su nacionalidad y se encuentre en situación irregular en el otro país o haya cruzado sus fronteras irregularmente.</p>

### ***¿CUÁLES SON LAS ETAPAS DEL CONTROL MIGRATORIO?***

En la práctica, el control migratorio es realizado por las instancias competentes a lo largo de cuatro etapas que se verifican en cualquier proceso de movilidad (23):

- 1) Etapa previa a la salida o ingreso
- 2) Etapa de control de ingreso
- 3) Etapa de control de permanencia
- 4) Etapa de control de salida.

Por ejemplo, un caso destacable en la región andina es el de Colombia, pues su legislación regula de manera diferenciada los controles de ingreso, permanencia y salida.



**¿CUÁLES SON LOS TIPOS DE CONTROL MIGRATORIO QUE SE EJECUTAN DURANTE ESTAS ETAPAS?**

En cada una de estas etapas, se aplican indistintamente hasta seis tipos de control migratorio o de la movilidad humana, como se verá en el siguiente cuadro (23):

<b>Tipo de control</b>	<b>Descripción</b>
Control de la buena fe y la habilitación de la persona que desea ingresar o salir del Estado	En esta etapa, se verifica que el motivo del traslado sea lícito y real (causa efectiva de la movilidad), y que no existan impedimentos de ingreso o salida. Es previo al traslado, y está asociado al otorgamiento de calidades o categorías migratorias, visados y documentos de viajes.
Control del cumplimiento de las condiciones y requisitos que permiten el ingreso al país en virtud de calidades o categorías migratorias específicas	Antes del ingreso al Estado, se verifica que la persona haya recibido una calidad migratoria. Esta puede basarse en el tiempo de permanencia: «no inmigrante», «inmigrante temporal» o «inmigrante permanente», «turista», o los demás previstos por los códigos de extranjería. La calidad migratoria también puede basarse en la actividad que se realiza en el país: religioso, estudiante, artista, etcétera. La suma de ambas fijan las condiciones para que una persona permanezca en territorio de un país del cual no es nacional.
Control de la autenticidad, vigencia y correspondencia de identidad de los documentos que sustentan su movilidad	Esta función se puede realizar en la etapa previa al ingreso o salida, o durante la permanencia (verificación de contratos de trabajo, de partidas de nacimiento, de documentos de identidad, etcétera), aunque con mayor rigurosidad se presenta en el ingreso.
Control de cumplimiento de las condiciones que autorizaron la permanencia de una persona en un determinado país	La autoridad competente supervisa y vigila que la persona que ha ingresado cuente con una autorización de permanencia vigente, que realice las actividades para las que se le autorizó y que subsistan los motivos que permitieron su ingreso.
Control de regularidad del ingreso y la legalidad del proceso de movilidad	Se verifica que el ingreso se haya realizado cumpliendo con los controles documentarios establecidos y no exista un acto ilícito de por medio (referido a la criminalidad asociada a la movilidad humana). En caso de irregularidad, la persona enfrentará sanciones administrativas y deberá iniciar un proceso de regularización. Frente a problemas relacionados con este tema, los funcionarios encargados del control deberían comunicar la incidencia a las autoridades competentes de la persecución del delito.
Control de la buena fe con que una persona realizó su proceso de movilidad	Implica la verificación de que la persona desarrolló su proceso de movilidad cumpliendo las condiciones de plazo y actividad que se establecieron al ingresar al territorio. Se realiza en la etapa de control de salida, es decir, cuando su estadía culmina. En caso se verifique que dichas condiciones no fueron respetadas, se aplicarán las sanciones administrativas (por ejemplo, el pago de

	multas o la prohibición de ingresos futuros) o sanciones penales previstas por ley
--	--

### **¿CÓMO SE ORGANIZAN LAS ACCIONES DE CONTROL MIGRATORIO?**

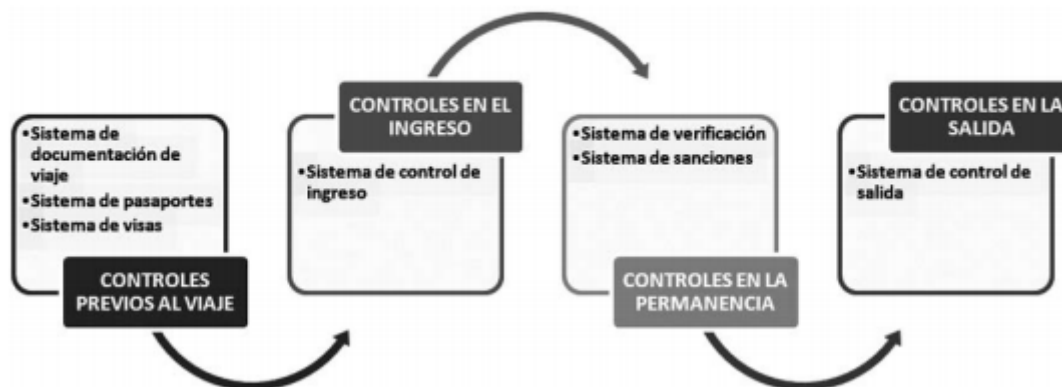
Las acciones de control migratorio se organizan en sistemas; que involucran la aplicación articulada de normas, procedimientos y prácticas de control. Los sistemas utilizados con más frecuencia son el sistema de visados, el sistema de pasaportes (de documentos de viaje), el sistema de control de ingreso, el sistema de verificación, el sistema de sanciones y el sistema de control de salida (23). En general, a cada una de las etapas del proceso de movilidad mencionadas en la Unidad I de este Módulo le corresponde un sistema de control. Sin embargo, en algunos casos, la atribución del Estado respecto de la aplicación de algunos de los sistemas se encuentra distribuida a lo largo de todo el proceso de movilidad.

#### Sistemas de control migratorio

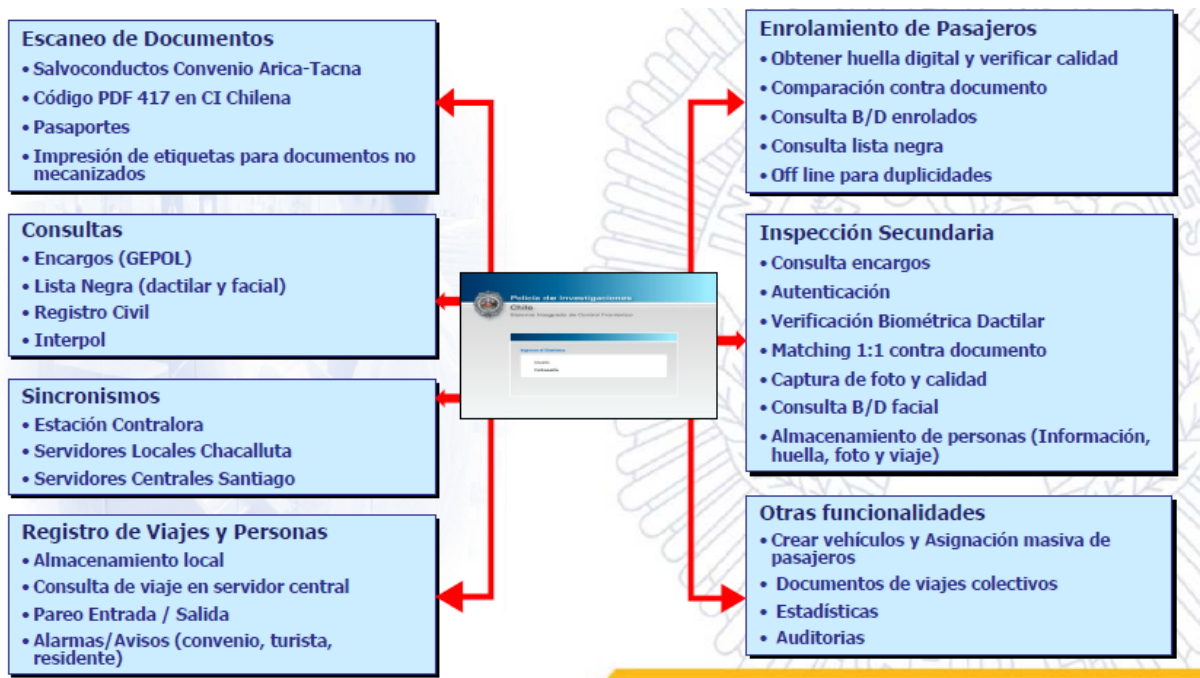
<b>Sistema</b>	<b>Descripción</b>
Sistemas de visas	La Visa es una norma emitida por un Estado para dar validez a la entrada de una persona a su territorio. Los Estados emiten visas como autorización de ingreso, como prueba del cumplimiento de los requisitos de admisión o simplemente como documento de identificación.
Sistemas de documento de viaje	Un documento de viaje tiene como función facilitar la identificación de los nacionales de un Estado para beneficio de los países extranjeros y para garantizar su derecho al retorno. Normalmente, se realiza a través de pasaportes, que son aceptados a nivel internacional.
Sistemas de control de ingreso «propiamente dicho»	Estos sistemas se aplican cuando la persona se presenta ante las autoridades en los lugares de control preestablecidos. Generalmente, este control implica actos por parte de un funcionario para i) verificar la buena fe y habilitación de la persona que desea ingresar; ii) certificar el cumplimiento de las condiciones y requisitos que permiten el ingreso; iii) verificar la autenticidad, vigencia y propiedad de los documentos que sustentan la solicitud de ingreso; y iv) comprobar las condiciones requeridas para el ingreso y la regularidad del proceso de movilidad.
Sistema de verificación de la condición de inmigración	Aplicado en la etapa de permanencia, implica i) supervisar y vigilar el cumplimiento de las condiciones (actividades, plazos, etcétera) que autorizan la permanencia de una persona en un determinado país; ii) verificar la regularidad del ingreso; y iii) verificar la legalidad (regularidad) del proceso de movilidad.

<p>Sistema de control De salida</p>	<p>Este sistema se aplica a las salidas voluntarias y a las motivadas por una sanción administrativa. Se implementa cuando la persona se presenta ante las autoridades para solicitar su salida del país. En estos casos, el Estado establece i) los lugares autorizados para la salida; ii) el tipo de documentación o requisitos, en caso sea posible; iii) el tipo de control que se puede realizar y los procedimientos permitidos; iv) los impedimentos de salida; y v) para los extranjeros, los mecanismos de retroalimentación, para obtener información que será evaluada en futuras solicitudes de ingreso. En este sistema, se debe verificar la habilitación de la persona que desea salir del país (si es nacional, no necesita autorización); la autenticidad, vigencia y propiedad de los documentos de viaje; la regularidad de la salida y la legalidad del proceso de movilidad.</p>
-------------------------------------	--

### Etapas y sistemas del control migratorio



**ELEMENTOS DEL CONTROL DE MIGRACIÓN AUTOMATIZADO**



Actualmente en el mercado se ha innovado mucho, contando con muy buenos sistemas de control de pasajeros en forma automatizada como es el caso de Chile que contempla las siguientes características (24):

Escaneo de Documento donde detecta en forma automática la información allí contemplada y el código pdf417 y la registra en el sistema, donde verifica los convenios ya existentes con países limítrofes (como es el convenio Arica-Tacna que permite ir de una ciudad hasta la otra sin utilizar pasaporte, solo con el documento).

Contempla también la lectura de los códigos contemplados en los pasaportes y una impresora que imprime un ticket para aquellos que no contemplan los documentos con dichos códigos para facilitar que los próximos movimientos migratorios sean más ágiles.

La información allí capturada es cruzada con la información contemplada por la policía local (gepol) contra listas negras dactilares y faciales, contra los datos contemplados en el registro civil y contra los datos contemplados en la interpol para garantizar un control más íntegro del movimiento migratorio.

Los puestos fronterizos siempre esta sincronizados con la estación contralora, como con servidores locales y/o centrales garantizando así la información centralizada y desatendida, registrando a las personas tanto a nivel local como a nivel central de forma

totalmente encriptado por posibles filtraciones de dicha información, como también las alarmas generadas por dichos controles.

También se efectúa la captura de las huellas digitales para identificar inequívocamente a los pasajeros como para efectuar los controles contra la información contemplada en el mismo documento, en bases de datos de listas negras nacionales e internacionales, o evitar movimientos duplicados con diferentes datos demográficos.

Y de requerirlo se complementa el control automático con una inspección secundaria donde se efectúa un control, uno a uno, por un Supervisor, quien contempla la verificación generada de la información biométrica de forma manual, captura foto facial y conjuntamente con el resto de la información ya capturada automáticamente complementa la información de la persona permitiendo así estadísticas y auditorías más fiables.

### **PREGUNTAS ACTUALES SOBRE LA BIOMETRÍA**

#### **¿Por qué hay tantas modalidades biométricas distintas?**

Cada aplicación y ambiente tiene distintas restricciones. Como ejemplo, vemos que muestras de huellas dactilares adecuadas requieren de la cooperación del usuario, mientras que una imagen facial puede ser capturada por una cámara de vigilancia. Asimismo, las huellas dactilares no están disponibles en muchos de los sospechosos en las listas de "buscados" (25).

También existe una multiplicidad de modalidades biométricas para distintas aplicaciones técnicas y razones financieras. Muchos científicos se interesan en el desarrollo de sistemas basados en su propia investigación. Luego de una implementación exitosa, gente con capital aventurera, interesados en la implementación de ese sistema, para comercializar el producto. Por lo tanto, amplias variedades de estas modalidades están siendo investigadas y varias ya están disponibles en el mercado.

#### **¿Puedo cambiar un aspecto biométrico de mi persona?**

Los aspectos biométricos biológicos no pueden cambiarse fácilmente (se han registrado casos de mutilaciones o huellas dactilares alteradas quirúrgicamente), pero pueden ser disimuladas. Si es posible cambiar un aspecto biométrico de comportamiento (25).

**¿Qué pasa si gemelos idénticos utilizan un dispositivo biométrico?**

Aunque así lo parezca, los gemelos idénticos parecen ser lo mismo al ojo humano, pero no lo son en lo que concierne a sus características biológicas y de comportamiento. Estas últimas presentan sutiles diferencias. Los métodos automáticos implementados en algunos de los dispositivos biométricos pueden generalmente identificar este tipo de diferencias sutiles y diferenciar dos gemelos aparentemente idénticos (25).

**¿La utilización de aspectos biométricos es segura?**

Los aspectos biométricos son típicamente pasivos y diseñados para mayor seguridad en su uso. Los sistemas biométricos usualmente implementan tecnologías de video y computación comunes, como pueden ser las que una persona encuentra en sus tareas del día a día (25).

**¿Los aspectos biométricos son una idea nueva?**

No, los métodos de reconocimiento humano han existido por siglos. El ejemplo más obvio es el del reconocimiento facial utilizado por los humanos. También, las huellas palmares fueron descubiertas al redor de inscripciones en cuevas, con una antigüedad estimada de 31.000 años, y se cree que son las firmas de los artistas. Sin embargo, los medios para automatizar tal información son prácticamente nuevos, con fecha en los principios de la década de 1960. El reconocimiento automatizado lo ha vuelto posible gracias, en las últimas décadas, gracias al avance de las capacidades de procesamiento de las computadoras y las comunicaciones (25).

Los aspectos biométricos de cada individuo varían en las distintas etapas de su maduración. El pasaje a la automatización de las huellas dactilares, como dijimos anteriormente, comenzó hacia finales de la década de 1960, mientras que en la automatización de las capturas de iris su historia se remonta sólo hacia algunas décadas atrás.

Muchos métodos, como ser el modo de caminar, continúan en etapas de investigación y desarrollo y no están listos aun para su despliegue formal.

**¿Son los métodos biométricos intrusivos?**

Esta es una pregunta subjetiva que podría ser respondida en formas distintas de acuerdo a las opiniones de distintos individuos. En general, la mayoría de las modalidades biométricas no son intrusivas, requiriendo únicamente el rozamiento de un dedo, una dirección de la mirada en la dirección que se solicite, o mencionar una proposición en voz alta. (25)

**¿Los sistemas biométricos son difíciles de utilizar?**

También es una pregunta subjetiva que depende de cada individuo. Aquellos usuarios que se encuentren más familiarizados con la tecnología electrónica tienden a tener menores inconvenientes con su utilización que aquellos que están menos familiarizados y que son escépticos a la utilización de tecnología. Desde una perspectiva operacional, la mayoría de las personas están capacitadas para utilizar cualquier dispositivo biométrico con muy poco entrenamiento. (25)

**¿Una vez que un aspecto biométrico de mi persona fue registrado, esos datos podrían ser utilizados en cualquier lugar donde esa tecnología específica sea utilizada?**

En general, no (25). Un aspecto biométrico registrado en un sistema no debería ser válido en otro sistema en el que esa tecnología para ese aspecto biométrico no sea utilizada. Sin embargo, si el sistema en el que un aspecto biométrico de una persona fue registrado está conectado con otro sistema afín, por ejemplo a través de una red, entonces sí, un aspecto biométrico de una persona puede ser aceptado en el lugar donde se ubique ese sistema alterno.

**¿Cuál es la diferencia entre la biometría y lo forense?**

Aunque tanto la biometría como la investigación forense implican el reconocimiento humano, la biometría es aplicada utilizando técnicas automatizadas específicas a la situación previa al evento, como podría ser el acceso a información sensible o a un área de máxima seguridad. Las aplicaciones forenses ocurren, usualmente, luego de que un crimen se haya producido y no utilizan métodos completamente automatizados. Los métodos forenses son aplicados para asistir en el proceso de adjudicación (legal). Las investigaciones forenses suelen tomar días de procesamiento (versus lo segundos que pueden demorar los métodos biométricos) y se atienen a requerimientos de precisión mucho más altos (25).



**¿Qué es la autenticación biométrica?**

"Autenticación Biométrica" es el término genérico que identifica el proceso de verificación. Dicho proceso involucra la presentación de una muestra biométrica para su consulta, comparación con un modelo o una plantilla almacenada en la base de datos y la determinación de si el individuo ha realizado una consulta legítima (25).

**¿Los aspectos biométricos se mantienen constantes a lo largo del tiempo?**

La permanencia de los aspectos biométricos varía según la modalidad. Por ejemplo, las huellas dactilares se mantienen constantes a lo largo de la vida de un individuo, exceptuando la utilización de superficies que poseen una prominencia a la degradación de la definición de los surcos. Las huellas dactilares están basadas en estructuras físicas dérmicas que se definen en el periodo fetal. Las cicatrices, temporales o permanentes, puede afectar los aspectos originales de la huellas, previos al nacimiento. El paso de los años, la vejez, afecta con mayor visibilidad a la cara. Estudios más detallados del efecto del paso del tiempo en otras modalidades no han sido desarrollados aun (25).

**¿Qué factores contribuyen al desarrollo de algún aspecto biométrico en una persona?**

Un aspecto biométrico esta principalmente afectado por su código genético único. Por otro lado, un aspecto biométrico de un individuo también se ve afectado por su ambiente. Por ejemplo, características del estilo de las huellas dactilares y de la estructura del iris son afectados por condiciones a las que se expone un feto en su ambiente prenatal (25).

**¿Cómo hacen los sistemas biométricos para determinar las coincidencias?**

Los sistemas biométricos pueden ser descriptos, aunque de un modo muy simple, en un proceso de tres pasos.

El primer paso en este proceso implica una observación o recopilación de los datos biométricos. Para ello utiliza varios sensores, que varían según la modalidad, para facilitar la observación.

El segundo paso, convierte y describe la información observada utilizando una representación digital llamada plantilla (o *template*). Este paso, también varía entre modalidades de diseño e incluso entre proveedores.



En el tercer paso, la planilla recién confeccionada, es comparada con una o más plantillas almacenadas en la base de datos. El resultado de esta comparación es una coincidencia o incompatibilidad y su resultado concreto es utilizado para acciones como, permitir el acceso, activar una alarma, etc. (25)

**VENTAJAS Y DESVENTAJAS DE LAS DISTINTAS MODALIDADES BIOMÉTRICAS**

**CARACTERISTICA ELEGIDA: HUELLA DACTILAR**

<u>VENTAJAS:</u>	<u>DESVENTAJAS:</u>
Los sujetos tienen múltiples huellas dactilares.	Las complicaciones privadas que conciernen a las implicaciones criminales.
Fácil de usar, con algo de entrenamiento.	Preocupaciones de salud o sociales en relación a tocar un sensor que es utilizado por incontables cantidades de personas.
Algunos de los sistemas requieren poco espacio virtual.	Una colección de imágenes de uña-a-uña requiere de entrenamiento y destreza, porque la tecnología de lectura básica actual es muy robusta
Grandes cantidades de datos existentes para permitir chequeos de antecedentes.	La edad de un individuo y su ocupación pueden producir algunas dificultades en el sensor para capturar una imagen dactilar completa y correcta
Ha probado su efectividad a gran escala de sistemas, a lo largo de los años de su uso.	
Las huellas digitales son únicas para cada dedo de cada individuo y la configuración de surcos se mantiene permanente durante toda una vida.	

**CARACTERISTICA ELEGIDA: ROSTRO**

<u>VENTAJAS:</u>	<u>DESVENTAJAS:</u>
No requiere contacto personal.	El rostro puede ser obstruido por el pelo, anteojos, sombreros, pañuelos, etc.

Sensores disponibles fácilmente (cámaras).	Sensible a los cambios en la luz, la expresión y la pose.
Grandes cantidades de datos existentes para permitir chequeos de antecedentes.	Los rostros se modifican conforme pasa el tiempo.
Chequeo fácil por parte de los humanos para verificar resultados.	Los usuarios son propensos a capturar imágenes de baja calidad aun esperando resultados de buena precisión.

**CARACTERISTICA ELEGIDA: IRIS**

<b><u>VENTAJAS:</u></b>	<b><u>DESVENTAJAS:</u></b>
No hay necesidad de tomar contacto físico.	La captura en algunos individuos es muy difícil.
Órgano interno y protegido, con menor preponderancia a lesiones.	Se la puede ocultar fácilmente con pestañas, parpados, lentes y reflejos de la córnea.
Se cree que tiene una alta estabilidad a lo largo del tiempo.	Mitos y creencias populares relacionadas con el prejuicio del escaneo del ojo desde una fuente de luz.
	La adquisición de una imagen de iris requiere de un mayor entrenamiento y una mayor atención que la mayoría del resto de los sistemas biométricos.
	No puede ser verificado por un humano.

**CARACTERISTICA ELEGIDA: VENAS**

<b><u>VENTAJAS:</u></b>	<b><u>DESVENTAJAS:</u></b>
Se percibe a menudo como menos invasor que otros sistemas biométricos.	Pero la carencia de pruebas a gran escala y de estándares, constituyen serios obstáculos a superar.
Todas las tecnologías de reconocimiento de venas trabajan de la misma manera. Se captura el patrón de la vena del individuo usando la luz del infrarrojo próximo.	El costo puede también ser otro factor, pues los dispositivos son más caros que los productos biométricos actuales para el control de acceso.
Las mayores ventajas de la biometría de las venas de la palma son el “anti hacking”, así como el hecho de que el usuario no tiene que tocar el dispositivo para utilizarlo.	

## EL PROBLEMA

Diariamente muchísimas personas y sistemas de control se enfrentan y resuelven el mismo problema: identificar a la persona que dice ser. La herramienta más utilizada para conseguirlo es la contraseña, pero claramente este es un método que se puede robar u olvidar, y por tal motivo no identifica inequívocamente a las personas o utilizarla para el control migratorio.

Debido a este motivo se ha desarrollado alternativas como la verificación mediante biometría, que puede utilizar nuestras huellas, rostro o nuestra voz, métodos que se han implementado hasta en los sistemas informáticos móviles, y por tal motivo también son las más expuestas a su adulteración. (26) Y frente a esto se presenta el siguiente problema: **las técnicas biométricas bien desarrolladas necesitan herramientas muy complejas y tienen un coste muy alto.**

La mayor diferencia entre un sistema ordinario de contraseñas y un sistema biométrico es que la muestra original y la muestra a verificar nunca coinciden a la perfección. No se pueden obtener dos huellas dactilares totalmente idénticas del mismo dedo y la situación empeora si usamos el rostro humano. Los rasgos faciales dependen de la luz, la hora del día, el maquillaje y, por supuesto, la edad. La voz, a su vez, también se ve afectada por múltiples factores como por ejemplo, un simple resfriado. Bajo estas condiciones, es realmente difícil desarrollar un sistema que permita el acceso al propietario; negándosele, a su vez, a los extraños.

Para resolver el problema, los sistemas biométricos intentan limpiar las muestras escaneadas de cualquier elemento que interfiera en el proceso de verificación, utilizando solo las características fácilmente reconocibles. Sin embargo, este “esqueleto” debe coincidir con el original según unos parámetros matemáticos. Para un sistema de seguridad medio, se asume como normal un margen de error de un extraño por cada 10.000 intentos y el bloqueo del usuario legítimo cada 50 casos. Pero para sistemas de control de migración dicho margen de error no es aceptable, dado la sensibilidad del asunto.

No existe una modalidad biométrica que sea mejor para todas las implementaciones. Muchos factores deben ser tenidos en cuenta al implementar un dispositivo biométrico, incluyendo la ubicación, los riesgos de seguridad, la tarea (de identificación o de verificación), cantidad de usuarios esperables, circunstancias de utilización, datos existentes archivados, etc. Es también importante notar que las modalidades biométricas están en distintas etapas de maduración. Por ejemplo, el reconocimiento por huellas dactilares ha sido utilizado por más de un siglo, mientras que el reconocimiento por iris no tiene más de una década de utilización. Debe tenerse en cuenta también que la madurez del dispositivo no está relacionada con cuál de ellos es el mejor, pero puede ser un indicador de las tecnologías que tienen mayor experiencia en la implementación. (27)

Las plantillas biométricas son la representación digital de una característica distintiva de un individuo, representan información extraída de una muestra biométrica y es lo que se compara en un sistema de reconocimiento afín.

Las plantillas varían de acuerdo a las distintas modalidades biométricas y sus oferentes. No todos los dispositivos biométricos están basados en planillas. Por ejemplo el reconocimiento por voz está basado en "modelos". La diferencia entre los modelos y las plantillas escapa el espectro de este escrito.

---

## CAPITULO 3

### PROCESO DE CONTROL DE MIGRACIÓN

En este contexto, el sistema de control migratorio es un pilar fundamental para cualquier Nación que contemple incorporar los conceptos de e-governance entre sus prioridades y busque implementar las mejores políticas para con sus ciudadanos basadas en datos fehacientes oportunos y obtenidos con las mejores tecnologías de información y comunicación.

Por dicho motivo contemplar el flujo migratorio de personas en el territorio de cualquier Nación, permite tomar las correctas decisiones para su administración y obtener los mejores beneficios de dicho flujo, sin ignorar evitar mediante el control exhaustivo el ingreso o egreso de personas no deseadas.

Dicho control debe estar contemplado en todos sus pasos fronterizos y/o aeropuertos y ríos donde se reciban y emigren personas del territorio nacional, **este sistema está pensado más allá de la república Argentina**, y considerando un complemento adecuado para un Estado/Republica que al contemplar principios de Gobierno Electrónico fomente una gestión de Gobierno Abierto y transparenten con idónea toma de decisiones en políticas de migración.

Pero fundamentalmente constituyen enfrentar una vulnerabilidad para la seguridad interna, por eso contemplar controles robustos que identifiquen inequívocamente a las personas mediante lectores de rostro e iris, autenticadores de documentos especializados, equipos de reconocimiento dactilar y de vasos sanguíneos para luego ser comparados con fuentes legítimas de información tanto internas como externas de forma online (y en su defecto offline), constituyendo la herramienta fundamental para aplicar medidas y estrategias que enfrenten con más eficacia los peligros emergentes de la delincuencia mundial.

Como hemos visto, la biometría es fundamental en todo sistema de control migratorio, para identificar en su movilidad migratoria a las personas, tanto nacionales como extranjeros, ésta provee de métodos de máxima seguridad y de gran utilidad en donde sea necesario un

nivel de seguridad o control que requiera la identificación de individuos, dado que se basa en rasgos que son distintivos en cada persona, que no sufren variaciones a lo largo del tiempo. No existen dos personas con la misma huella y/o rostro.

Brindar un mecanismo de registración altamente confiable, que combinado con el uso de firma digital permite en consecuencia la eliminación del soporte papel del movimiento migratorio de Entrada o Salida. Posibilitando en un mismo lapso de tiempo, no solo controlar la documentación de una persona de forma automática, sino también controlar su huella dactilar, venas, rostro e iris. Y al registrar dicho movimiento garantiza que ante un eventual reclamo administrativo y/o judicial pueda acreditarse la identidad del pasajero de forma rápida y precisa.

Para comenzar con el control de la documentación, primero debemos contemplar una base de datos unificada y replicada en cada puesto de control, dichos puestos de control estarán ubicados remotamente en diferentes puntos geográficos donde se requerirá conexión a la central. Evaluar que por índoles de la naturaleza o factores externos, dicha comunicación puede ser interrumpida momentáneamente, por tal motivo se aconseja establecer una copia encriptada central en un puesto de control actualizada regularmente con todos los movimientos migratorios registrados para permitir verificar la información de un pasajero sea contemplada allí y comparada en cada nuevo movimiento del viajero, como también en dicha base de datos se incluirá las listas propias de Personas y Documentos en Black List generada por el propio gobierno contralor.

Para lo cual se implementará una Network Load Balance (NLB) permitiendo que los servidores de los puntos de control siempre estén sincronizados con el servidor central unificado, dicha tecnología está disponible con la licencia de Microsoft Server desde la versión 2008 por tal motivo no requiere licencia adicional, Esta tecnología permite implementar un esquema de alta disponibilidad donde se define un clúster de equipos (NLB clúster) que posee asignada una dirección IP virtual y dos o más nodos de este clúster cada uno con su propia IP y otra IP dedicada a la comunicación dentro del clúster. De esta forma, las solicitudes de los clientes son enviadas a la IP virtual del clúster y el servicio de NLB en cada nodo se encarga de distribuirla entre los equipos. Si un nodo sale de línea, los otros

toman su lugar, por lo que el servicio que implementen los nodos del clúster está siempre disponible mientras exista al menos 1 nodo activo.

La decisión sobre que nodo del clúster atiende cada pedido deberá ser realizada de acuerdo a algoritmos que consideran la dirección IP del cliente, de ahí el nombre de la tecnología de Network Load. Se pueden configurar distintas alternativas de acuerdo a los requerimientos y al tipo de servicio que se define para la alta disponibilidad.

NBL es especialmente apropiado para dos entornos de aplicaciones: Terminal Server y granjas de servidores web (web farms). (28)

## LECTOR DE PASAPORTES ELEGIDO: REALPASS-V



Una vez garantizada la disponibilidad mediante esta tecnología de la base de dato con los registros de movimientos migratorios anteriores y black list propias y mantener siempre actualizada la aplicación, procedemos a efectuar el escaneo automatizado de la documentación garantizando en un 95 % la integridad de que el mismo no fue adulterado. Esto se puede efectuar por una puerta biométrica con lector de pasaportes incluido o dicho lector de pasaporte en forma individual manejado por un Inspector dedicado. En base a sus ventajas se decide por éste último contemplando el RealPass-V es el más versátil por las siguientes ventajas (29):

- Lectura en un solo paso de **datos de la página completa y chip de documentos** y tarjetas ICAO estándar.

Usando esta técnica el lector de pasaportes RealPass tarda solo un segundo en



capturar los datos y mostrarlos por pantalla con luz blanca e infrarroja (modelo Suprema RealPass-V RPV-RU).

- Escaneo de documentos **fácil y rápido** de usar

Para cuando la velocidad importa el diseño de la superficie de colocación de documentos asegura el escaneo rápido y preciso.

- **Rápida velocidad de reconocimiento** y baja tasa de error en la lectura de caracteres OCR y datos del chip.

Los lectores de pasaporte Suprema procesan los datos ópticos, gráficos y RFID de documentos estándares como los doc ICAO 9303 y MRTD con protocolos de seguridad BAC, PA, AA, EAC (CA, TA). También está equipado con iluminación UV y Infrarroja para soportar aplicaciones de alta seguridad. Bajo la luz UltraVioleta se pueden observar diferentes trazos de seguridad invisibles.

- Sin partes movibles o extraíbles, **mínimo coste de mantenimiento**



**CARACTERÍSTICAS DEL REALPASS-V**

- Lee la página completa (incluyendo imágenes y zona de lectura mecánica en líneas 1, 2 y 3) y chip RFID de documentos y tarjetas de viaje en conformidad con OACI Documento 9303

- Captura la imagen del documento con resolución de 400dpi y 24 bits de color

- Permite extraer y almacenar imágenes específicas del documento, como la fotografía o firma



- Óptica de múltiples lentes para lectura mejorada

- Iluminación infrarroja o ultravioleta para la detección de elementos de seguridad en el documento

- Lee tarjetas con chip contactless ISO 14443 Tipo A/B

- Soporta los protocolos de seguridad de pasaportes electrónicos: BAC (Basic access control), PA (Passive authentication), AA (Active authentication) y EAC (Extended access control, opcionalmente)

- Protector removible para limpiar la ventana de lectura

- LED multicolor y sonido para una interface de usuario intuitiva

- Interface USB 2.0 de alta velocidad

- Control de calidad para la emisión de pasaportes opcional

- Lectura de códigos de barra 1D y 2D opcional

- SDK para integración eficiente en cualquier sistema

**CONCEPTOS TEÓRICOS EN LOS CUALES SE RESPALDA**

El RFID es en esencia un identificador basado en radiofrecuencia. Podríamos definirlo como una herramienta tecnológica de identificación cuya principal premisa es sustituir al código de barras actualmente existente. Dicha tecnología ofrece un sistema único de localización en tiempo real que permite monitorizar además cualquier parámetro referente al objeto que la comporte. (30)

Existen estándares RFID que se encargan de regular la comunicación entre tags y readers, comunicación de tipo RF con propagación en el medio aire. Se regulan además las estructuras de datos (organización, formato, etc.), la compatibilidad con los estándares de esos datos, y las aplicaciones (y como los estándares se adaptan a estas).

La ISO (The International Organization for Standardization) ha creado una serie de estándares para RFID:

- La norma ISO 11784 define como se estructuran los datos en el tag.
- La norma ISO 11785 define el protocolo en el interfaz aire para los tags utilizados en sistemas de pago y tarjetas inteligentes sin contactos (ISO 14443).
- Para testear la compatibilidad y el cumplimiento del estándar, la norma ISO 18047 fue creada, ampliada por otra norma, la ISO 18046, que regulaba las distintas evaluaciones de rendimiento que se puede hacer a tags y readers.

El pasaporte biométrico, también conocido como pasaporte electrónico, es un documento de identidad que

además del uso de papel de seguridad, contiene una lámina de policarbonato con un circuito electrónico incrustado en ella, y que usa la biometría para autenticar la ciudadanía de los viajeros. La incorporación de un minúsculo chip RFID en el documento permite tanto almacenar información adicional como duplicar la que se encuentra impresa en la página que contiene los datos del titular del pasaporte, permitiendo -a través de Infraestructura de clave



pública- la certificación de la veracidad de los datos contenidos en él, haciendo virtualmente imposible forjar identidades falsas. (31)

La descripción del documento, así como las características del chip se hallan descritas en el Documento 9303 de la Organización bajo la denominación "Documentos de viaje de lectura mecánica"

El Pasaporte Electrónico suele contemplar las siguientes Medidas de seguridad que complementan la información del Chip RFID para su autenticidad, como es el ejemplo del pasaporte Español que hoy en día es el referente en medidas de seguridad. (32)

Contempla una Cubierta con Sobreimpresión fluorescente en amarillo del escudo y el nombre del país que lo emite y medidas de seguridad visibles bajo la luz ultravioleta en dicho escudo. En la contraportada también contempla dicho escudo sobreimpreso con tinta fluorescente amarilla visible bajo la luz ultravioleta pero complementa dicha contraportada con técnicas de microimpresión como muestran las siguientes imágenes:



En la página de datos personales hay un hilo de seguridad con texto que contempla el carácter único de pasaporte, se encuentra la misma foto como marca de agua debajo de los datos personales, la misma contempla un laminado de seguridad con hologramas ópticamente variables y mantiene medidas de seguridad visibles bajo la luz ultravioleta como fibrillas fluorescentes en azul y amarillo, en las páginas interiores replica dicho hilo de seguridad con texto indicativo y las fibrillas fluorescentes claramente visibles bajo la luz ultravioleta y se le agrega diferentes marcas de agua como numeración por perforado láser en todas sus hojas que garantiza ninguna de ellas sean reemplazadas.



También se contemplan en diferentes pasaportes características como Impresión calcográfica en dos colores, imágenes latentes, micro textos, tintas ópticamente variables, marcas de agua multifocal, guillotes en varios colores, impresión offset de seguridad, trampas especiales de seguridad y tintas invisibles a simple vista.

RealPass-V es un lector compacto de pasaportes biométricos que lee con precisión los datos del pasaporte estándar OACI 9303 en un solo paso sin la necesidad de leer el pasaporte varias veces. El lector combina el procesamiento de datos gráficos y ópticos, y el chip de RF con protocolos de seguridad estándares OACI para lograr un gran nivel de seguridad.



RealPass-V está equipado con una función de iluminación IR y UV para aplicaciones de alta seguridad. Bajo la iluminación UV, aparecen hilos de seguridad invisibles de varios colores para que el usuario pueda verificar la información. La detección automática de documentos está asegurada por el procesamiento de gran volumen a alta velocidad, la lectura en un solo paso, el ajuste optimizado de una antena de RFID y una interfaz USB 2.0.

RealPass-V cuenta con un diseño tipo plano para un escaneo de documentos rápido, constante y preciso. Además, el dispositivo no incluye piezas movibles, lo que lo hace resistente y necesita un costo de mantenimiento mínimo luego de la implementación y el despliegue en el campo.

**\* Contenido de Manual SDK del RealPass-V; Descripción de los Componentes y Especificaciones Técnicas serán contempladas en el Anexo F del documento.**

## LECTOR DE HUELLAS DIGITALES ELEGIDO: REALSCAN-G10

Considerado por contemplar la certificación IAFIS Apéndice F del FBI que garantiza a los usuarios que los productos cumplen o exceden los estándares de interoperabilidad del FBI y funcionan con el Integrated Automated Fingerprint Information System (IAFIS, Sistema Integrado Automático de Información de Huellas Dactilares). Asegura que las imágenes utilizadas son de la más alta calidad y son compatibles con todas las fases de identificación para expertos en huellas dactilares y el IAFIS. El Apéndice F tiene estrictas condiciones de calidad de imagen, que se centran en la comparación de huellas dactilares humanas y facilita una operación de reconocimiento "muchos a muchos" (many-to-many) de la máquina a gran escala. (33)



RealScan-G10 cuenta con la avanzada tecnología de construcción de imagen capturada por medio del algoritmo único de detección fuera de foco de Suprema para construir imágenes de las huellas dactilares enroladas. Con la tecnología ARIC, RealScan-G10 realiza capturas a más de 20 fotogramas por segundo, lo que garantiza la máxima calidad de imagen y un bajo índice de errores. Los intuitivos iconos gráficos indican qué tipos de huellas escanea el dispositivo y las luces LED en la punta de los dedos indican cuándo se deben poner los dedos. Los botones de funcionamiento en ambos lados ayudan a los usuarios a operar el escaneo directamente desde el escáner y el altavoz incorporado permite instrucciones de voz totalmente programables.

**CARACTERÍSTICAS DEL ALGORITMO VERIFINGER UTILIZADO POR REALSCAN-G10**

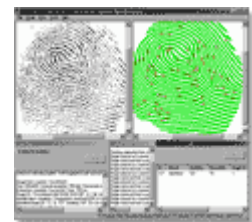
VeriFinger fue desarrollado en 1998, es un algoritmo de identificación de huellas dactilares diseñado para integradores de sistemas biométricos. Desde entonces se ha convertido en el más poderoso algoritmo de reconocimiento dactilar que existe hasta hoy. La última versión 7.1 es compatible con NIST MINEX, basada en el motor MegaMatcher que ha sido certificado por NIST para aplicaciones de verificación de identidad personal (PIV). VeriFinger sigue el esquema comúnmente aceptado de identificación dactilar, que utiliza un conjunto de puntos específicos de la huella (minucias) junto con soluciones algorítmicas propietarias que mejoran el rendimiento y confiabilidad. (34) Algunas de esas soluciones se mencionan a continuación:



- **Comparación de huellas planas y roladas.** VeriFinger compara huellas plana-rolada, plana-plana o rolada-rolada con alta confiabilidad por ser tolerante a deformaciones. Las huellas roladas tienen una alta deformación debido a la técnica de captura (rotar el dedo desde un borde al otro) respecto a las huellas planas. Los algoritmos convencionales, comparan huellas roladas de forma menos confiable debido a estas deformaciones.

- **Tolerante a traslación, rotación y deformación.** VeriFinger identifica huellas aún si están rotadas, reposicionadas, deformadas o si coinciden 5-7 puntos (suelen coincidir 20-40 puntos) y compara hasta 40,000 huellas/seg.

- **Capacidad de identificación.** VeriFinger puede comparar 1-a-1, y 1-a-N



- **Detección de calidad.** VeriFinger es capaz de garantizar que sólo las plantillas dactilares de mejor calidad sean ingresadas a la base de datos utilizando esta función durante la captura.

- **Filtro adaptivo de imágenes.** Elimina ruidos, ruptura y bloqueo de crestas para una extracción confiable de minucias - incluso en imágenes de baja calidad - con un tiempo de proceso de 0.6 segundos. Esta captura de pantalla de la aplicación demo



VeriFinger muestra la imagen inicial de una huella plana (ventana izquierda), y la misma imagen después filtrar y procesar el ruido por VeriFinger, con la posición y dirección de las minucias marcadas con líneas y círculos rojos.

- **Modo de captura generalizada.** Esto crea una colección de características dactilares a partir de varias imágenes del mismo dedo. Cada imagen se procesa y se extraen sus características. Luego se analiza el conjunto y se combina en una sola colección. Así, las características almacenadas son más confiables y aumenta la calidad del reconocimiento.

- **Algoritmo de optimización para escáneres.** VeriFinger 7.1 incluye funciones que ayudan a lograr mejores resultados para los escáneres compatibles.

**\* Contenido de VeriFinger 7,1; Descripción de los Componentes Dactilares y Especificaciones Técnicas serán contempladas en el Anexo A del documento.**

**\* Contenido de los controles AFIS y Multibiométrica para proyectos de gran escala; Descripción de MegaMatcher 5.1 y Especificaciones Técnicas serán contempladas en el Anexo D del documento.**

## RECONOCIMIENTO DE ROSTRO E IRIS ELEGIDO: ICAM TD 100

ICamTD100 con Iris ID ha sido el producto comercial con más reconocimiento en el mercado desde 1997, debido a su algoritmo de reconocimiento del iris. En miles de lugares, IrisAccess @ autentica la identidad del iris de más personas que todas las demás plataformas combinadas de reconocimiento de iris. La amplia experiencia de IrisID en el reconocimiento del iris se ejemplifica en el TD100 ICAM, que incluye un sistema óptico especialmente diseñado y optimizado para funcionar en perfecta armonía con la alta velocidad integrando una matriz multi-sensor de imágenes de iris. El ICAM TD100 automáticamente procesa y regresa imágenes de alta calidad compatible con los estándares ISO de imágenes de iris de un sujeto en menos de un segundo mientras el dispositivo o el sujeto se aproxima a la distancia óptima de captura. (35)



InSight o Duo proporciona la potencia combinada de datos biométricos del iris y rostro en un solo dispositivo delgado. Y con un tiempo de captura de 6 segundos cumpliendo con los estándares en captura de rostro y la doble imagen del iris, a una distancia de 2 metros, el InSight Duo ofrece un rendimiento excepcional sin comprometer el alto rendimiento del sistema original Insight. Además proporcionando un cumplimiento de ADA (American with Disabilities Act) para capturar en volumen, lo que permite la captura de la imagen del rostro e iris sin esfuerzo y de cualquier persona si están en una silla de ruedas o por encima de los 7 pies (2,15 metros) de altura.

Uno de los puntos más importantes, de cara a los usuarios, en un sistema de reconocimiento es la privacidad. En un sistema de estas características, se construyen plantillas biométricas de los usuarios con el fin de poder compararlas posteriormente. De ahí que sea vital que dichas plantillas permanezcan seguras 100% ya sean en el servidor o en el propio dispositivo.

Sin embargo, siempre existe el riesgo de ver comprometidas las credenciales de usuario en caso de pérdida o robo del dispositivo, o bien por alguna brecha de seguridad en el caso de los servidores. Para solucionar esto, IrisID tiene como premisa fundamental no



almacenar nunca los patrones biométricos obtenidos del usuario. Esto es posible gracias a técnicas de encriptación biométricas.

iCam TD100 Proporciona las siguientes características:

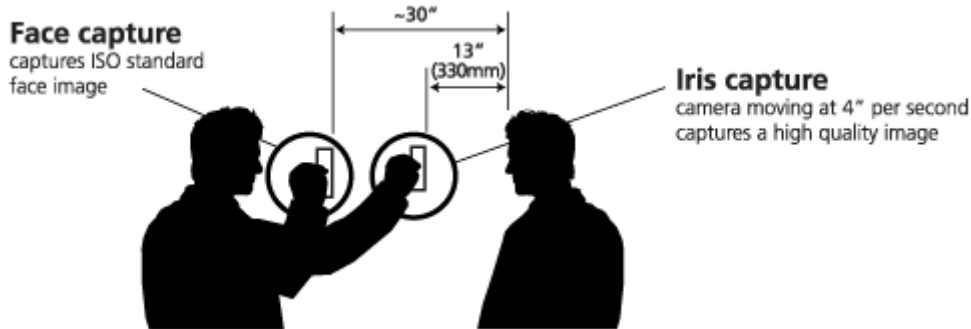
- Captura de alta velocidad Dual Iris
- Compacto y ligero
- Movimiento Individual de Iris automático y captura de rostro
- Sistema de guía del operador intuitiva
- Cumple Normas de estándares Hardware y Software

### **ALTA VELOCIDAD - CAPTURA DUAL IRIS**

El ICAM TD100 incluye un sistema óptico diseñado y optimizado para funcionar en perfecta armonía con la alta velocidad de los múltiples sensores de iris que captan imágenes de forma integrada. El ICAM TD100 procesa automáticamente y cumple con estándares ISO de alta calidad de imágenes capturando el iris de un sujeto en menos de un segundo, por más que el dispositivo o el sujeto se encuentren en movimiento de aproximación a la distancia óptima de captura.

### **PROCESO DE CAPTURA DE IMAGEN DE IRIS**

Las rutinas de captura de imagen del iris y doble análisis de la calidad son totalmente automáticas y están disponibles como parte del conjunto de API Iris Identificación SDK para la aplicación en el campo de la ICAM TD100. Una ilustración de la pantalla de captura de iris se muestra a continuación. Iris y la captura de la cara mediante NEO FACE se llevan a cabo por el operador de la ampliación de su brazo desde la distancia de captura de cara a la distancia de captura de iris como se ilustra a continuación. (36)



**La API - función de captura neo-face**

- La función de encuadre integrada proporciona información para la captura de imagen de la cara en formato ISO / ICAO.
- Captura NEO-FACE Manual con enfoque automático también permite a través de las diferentes llamadas a la cámara desde la aplicación por ejemplo iData SDK.
- Un desarrollador de aplicaciones también puede utilizar el protocolo basado en la Host-Face para activar la captura NEO-FACE de forma automática desde el procesador anfitrión.
- Captura facial se puede iniciar a través de la API o mediante el botón del obturador en el ICAM TD100.
- Ilustraciones de ejemplo de los modos de captura cara se muestran a continuación.



---

**CONCEPTOS TEÓRICOS EN LOS CUALES SE RESPALDA**

La estructura vascular de la retina es supuestamente diferente para cada individuo y cada ojo. La captura de este rasgo biométrico es compleja ya que requiere cooperación por parte del usuario y contacto con el sensor, lo cual compromete seriamente su aceptabilidad (por eso el dispositivo seleccionado que efectúa dicho análisis de rostro e iris sin contacto físico es la mejor opción en el mercado).

Los modelos de autenticación biométrica basados en patrones oculares se suelen considerar los más efectivos. Para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo cual dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver. (37)

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación. El hecho de mirar a través de un binocular (o monocular) no es cómodo para los usuarios, ni aceptable para muchos de ellos. Los usuarios no se fían de un haz de rayos analizando su ojo, y por otro lado un examen tan exhaustivo de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.

Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial (aparte del hecho de que la información es procesada vía software, lo que facilita introducir modificaciones sobre lo que nos han provisto para que un lector realice otras tareas de forma enmascarada).

**\* Contenido de VeriEyer SDK, Descripción del algoritmo y Componentes Biométricos serán contempladas en el Anexo B del documento.**

**\* Contenido de VeriLook SDK, descripción del algoritmo, capacidades, contenidos y componentes serán contemplados en el Anexo C del documento.**

## RECONOCIMIENTO DE VENAS ELEJIDO: PALMSECURE

PalmSecure es un dispositivo de autenticación biométrica que proporciona el más alto nivel de seguridad mediante la tecnología de autenticación de venas de la palma. Esta tecnología es ahora capaz de ser utilizado en una amplia gama de situaciones gracias a reducciones en el tamaño, reducciones en el costo, y la simplificación del desarrollo (38).



- **Sin contacto:** Debido a su función sin contacto, es muy higiénico y libre de estrés para su uso incluso público.
- **Fácil de usar:** Sólo tienes que pulsar la palma sobre el dispositivo, que captura el patrón de la vena al instante.
- **Autenticación Avanzada Precisión:** La autenticación de venas de la palma da cuenta con exactitud y autenticación avanzada, porque el patrón de venas de la palma tiene muchas y de gran tamaño de los vasos sanguíneos. Falso Rechazo Rate: 0.01%, tasa de falsa aceptación: 0,00008%
- **Alta seguridad y aplicabilidad Rate:** Difícil de falsificación de los datos de las venas de palma, ya que está dentro del cuerpo. Casi todo el mundo puede utilizarlo.
- **Opciones de hardware:** Los siguientes dos tipos de sensor PalmSecure™ están disponibles.
- **Las herramientas de desarrollo están disponibles:** Desarrollo de productos que integran el sensor PalmSecure™ se simplifica al adquirir el SDK.

Palm Secure escanea nuestra mano utilizando rayos casi-infrarrojos, permitiendo que la sangre absorba parte de estos rayos, que crean un patrón negro de todas las bifurcaciones venosas de nuestra mano. Ese laberinto de venas, único en cada ser humano, es el criterio de diferenciación que usa la Palm Secure.

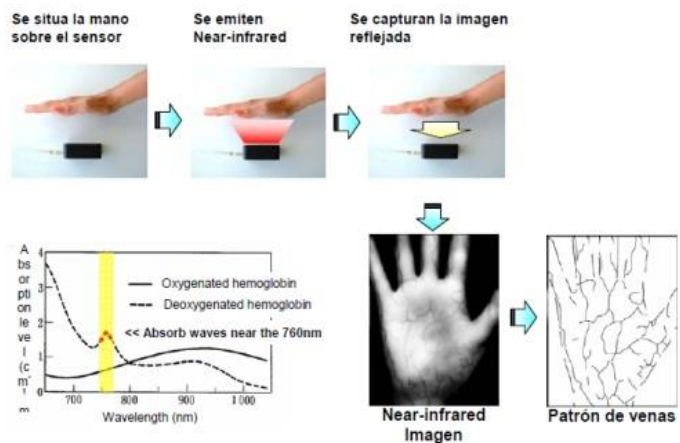
Por otra parte, PalmSecure es muy fácil de usar y no necesita ningún tipo de contacto físico, lo que la vuelve casi única. La implementación y los alcances de la Palm Secure son infinitas y apuntan a mercado tan disímiles como la seguridad personal, financiero/banca, control de accesos, asistencia médica, aplicaciones del gobierno, industria del automóvil, acceso a ordenadores, etc.

**PRINCIPALES CARACTERÍSTICAS:**

- Más compacto, con un sensor que mide tan solo 35x35x27mm
- Autenticación más rápida
- Rango de temperatura de operación más amplio
- Mejor integración en PCs
- Trae un completo kit de desarrollo (SDK) que incluye ejemplos de aplicaciones y herramientas de evaluación de la velocidad de autenticación

El nuevo PalmSecure ofrece una velocidad de autenticación extremadamente más rápida, un tamaño de 35mm x 35mm que es la cuarta parte del sensor original, un mayor rango de temperatura de trabajo y un coste inferior. La menor superficie del sensor proporciona una mayor flexibilidad y facilidad de implementación en las aplicaciones actuales, incluyendo ordenadores, cajeros automáticos y sistemas de control de acceso, a la vez que amplía en mucho el rango de nuevas aplicaciones potenciales, por ejemplo en áreas tales como copiadoras y otros equipos de oficina, historiales médicos electrónicos y otras soluciones que demandan una muy alta seguridad de autenticación. (39)

Funcionamiento del sensor "Palm Vein"



Entre los distintos productos que configuran la oferta de Palm Secure, se encuentra un SDK de desarrollo que incluye un Kit Palm Secure y un conjunto de librerías que incluye ejemplos de aplicaciones y herramientas para evaluación de la velocidad de autenticación.

La tecnología “Palm Secure”, captura una imagen del tramado de las venas de la palma de la mano a través del reflejo de rayos casi-infrarrojos emitidos. Esto es gracias a que la hemoglobina desoxidada de la sangre absorbe parte de estos rayos reduciendo de este modo el ratio de reflexión, ocasionando que las venas aparezcan como un patrón negro en la imagen capturada.

Las venas son elementos internos del cuerpo humano y tienen gran abundancia de múltiples e infinitas características que las diferencian, asumir una falsa identidad falsificándolas es extremadamente difícil, teniendo en cuenta que la sangre ha de estar fluyendo para registrar la imagen o patrón. Además, las investigaciones de Fujitsu demuestran que el patrón de las venas es único en cada individuo, incluso en el caso de gemelos idénticos, así mismo son diferente las venas en la mano derecha que en la izquierda. También hay que tener en cuenta que el patrón de las venas no cambia con el crecimiento, simplemente se amplía manteniendo el mismo patrón. (40)

La combinación de estos factores hace que el sistema de autenticación de Fujitsu, “Palm Secure”, sea un gran avance en soluciones de identificación biométrica, siendo el más alto nivel de seguridad en la identificación de personas del mercado.

Adicionalmente a este alto nivel de seguridad, la tecnología de Fujitsu es extremadamente fácil de usar y no necesita contacto físico, lo que la convierte en la solución idónea e higiénica para su uso en sistemas de identificación de múltiples usuarios. El usuario únicamente tiene que poner la mano encima del escáner a una pequeña distancia y éste automáticamente procede a la autenticación.

## **POTENCIAL**

Utilizando tecnología Palm Vein, el Palm Secure es un dispositivo que cuenta con un sensor muy particular: se trata de una suerte de escáner que conduce una luz semi infrarroja, la cual se encarga de leer el conjunto de venas y arterias de la mano. (41)

De inmediato lo codifica, a partir de un algoritmo propio de Fujitsu, y lo compara con la información que ya está registrada.

La clave está en que, para validarla, “la mano tiene que estar viva”, aclaró el Country Manager de Fujitsu para Latinoamérica, Juan Ignacio Accogli, con quien la empresa inició sus operaciones desde la oficina en Argentina, que a su vez abrió en abril de 2011.

Esto explica por qué uno de los principales mercados potenciales de este producto se relaciona con la banca y finanzas, por ejemplo, para la llamada “prueba de vida” que exigen las cajas de jubilaciones en países como Argentina.

El ejecutivo explicó que un cajero con Palm Secure evitaría que la persona tenga que presentarse a la caja cada 90 días, como exige la ley en ese país. Si la persona realizó una transacción en un cajero con esta tecnología, por ejemplo, “ya está considerado como prueba de vida”.

Además de este sector el Palm Secure es requerido por centros de procesamiento de datos (*datacenters*) para el control de acceso, así como para la validación de clientes VIP para el acceso a caja y en laboratorios con acceso a fármacos.

Agregó que el mercado también se extiende a hospitales y universidades. Por ejemplo, en Japón se utilizan para la identificación de pacientes en ambulancias y en Estados Unidos se emplea para el reconocimiento de los alumnos a la hora de rendir exámenes.

### **LA PALMA VERSUS EL DEDO**

Una de las ventajas con las que cuenta Palm Secure frente a otros sistemas de identificación biométrica, como el de huella dactilar, es que “el mapa de venas y arterias no se modifica con el transcurso de la vida”, explicó Accogli. Aseguró que a las personas que realizan trabajos fabriles, o que trabajan en la industria química, por ejemplo, la huella dactilar puede llegar a borrárseles o incluso puede formarse un callo que haga que la huella no pueda leerse.

**Una de las ventajas frente al sistema de huella dactilar es que el mapa de venas y arterias no se modifica con el transcurso de la vida”, explicó Accogli (42)**

Por otro lado, como no se exige contacto físico con el sensor se trata de un sistema más higiénico, además de inocuo.

Además, en determinados segmentos de la población puede existir resistencia al sistema de la huella dactilar, ya que “lo asocian con el registro policial”, añadió el ejecutivo.

No obstante, un punto a favor del viejo sistema es ser más económico: “Así como Palm Secure es una tecnología superior, también es cierto que es más caro que un lector de huellas digitales o cualquier otro tipo de sistema de validación”.

Un dispositivo Palm Secure cuesta unos US\$ 600, aunque el precio total dependerá “del proyecto, de la solución”, que se mide sobre todo por las horas que el cliente quiera asignar.

Una forma de agilizar el proceso es montar el software de Palm Secure sobre otro de control de acceso. Para eso, cuenta con un kit de desarrollo de software que “se puede interface con casi todos los software de control de acceso del mercado”, señaló así Accogli otra de las ventajas del producto.



En un mundo hiperconectado, las tecnologías Human Centric ofrecen una oportunidad sin precedentes para co-crear servicios que los clientes y sus stakeholders demandan, pero que sólo la privacidad es protegida y los datos son seguros. Con Palm Secure, la multinacional nipona se convierte en el perfecto socio para complementar el conocimiento del negocio de sus clientes, gracias a su tecnología de autenticación, experiencia y soporte. Así y como por ejemplo al personalizar un dispositivo ID Match, similar a un punto de venta, se consigue una alta seguridad de autenticación de identidad bajo una solución fácil de usar. (43)

Los consumidores, ciudadanos y compradores están más abiertos a nuevas formas de relacionarse con creciente ecosistema digital de proveedores de servicios financieros, agencias del sector público y retailers. Modelos de “negocio distribuido”, están emergiendo y donde los límites organizacionales tradicionales y la cooperación a través de fronteras organizativas y geográficas, se han convertido en algo sencillo. Sin embargo, en este nuevo mundo la seguridad se vuelve, en consecuencia, más importante. Habilita una estrecha cooperación e innovación de servicios. Siempre que sea posible, se mantiene un estricto control de acceso, datos y pago.

**\* Contenido de Fujitsu PalmSecure; Descripción de los Componentes y Especificaciones Técnicas serán contemplados en el Anexo E del documento.**

## CAPITULO 4

### OBJETIVOS DEL PRODUCTO

Efectuar el control fronterizo mediante puestos equipados con la última tecnología en captura de biometría para identificar inequívocamente a cada pasajero y complementar la identificación con la captura automática de los documentos de viaje mediante tecnología que permiten no solo automatizar, sino también permita verificar la autenticidad de ellos.

Complementar dicha identificación de forma manual, y conjuntamente con las alertas automáticas y manuales posibles de los controles efectuados, poder derivar a una supervisión al pasajero por parte de personal especializado quien complementará dichos controles de forma manual e ingresará en el sistema firmando digitalmente los resultados de dichos controles.

Poder configurar las Business Rules y tablas necesarias para el funcionamiento de la aplicación de manera óptima y dinámica respecto a posibles futuros controles adicionales hoy no contemplados.

Administrar usuario de forma inequívoca aplicando las mismas tecnologías utilizadas para la identificación del pasajero permitiendo parametrizar si dichos usuarios solo contemplarán una clave de identificación o también deberá contemplar el control de las huellas para su identificación e ingreso al sistema.

Administración de dependencias coincidentes con los puestos fronterizos donde se identificará mediante la asignación de su correspondiente IP y catalogará la modalidad del puesto de trabajo (entrada o salida) correspondiente a un tipo de transporte (aéreo, fluvial o terrestre).

El sistema deberá:

- Organizar y controlar la entrada y salida de personas nacionales o extranjeras.
- Unificar registros de datos migratorios de los distintos puestos de frontera.

- Permitir consultar en tiempo real la información sobre personas que ingresan y salen del país.
- Contar con Recursos tecnológicos que permitan el registro, almacenamiento y gestión de la base de datos biométricos, demográficos y documentación de viaje.
- Conexión con Web Services Externos.

### **DESCRIPCIÓN FUNCIONAL**

Registro de Ingreso / Egreso del pasajero, a través de los distintos medios que se dispongan (aéreo, marítimo y/o terrestre) registrando

- Datos personales
- Escaneo del pasaporte
- Captura de datos biométricos
- Últimos movimientos registrados para el pasajero
- Chequeo contra listas negras
- Validación de menores
  
- Validación de VISAS
  - Chequeo Automático por Visa requerida a través del tipo de documento de viaje y la nacionalidad del pasajero
  - Registro de los datos de Visa en caso de corresponder
  - Chequeo de la validez de la Visa a través de los lectores de documento de viaje.
  
- Listas Negras
  - Administración de Listas Negras de Personas (registradas a través de nombre y/o fecha de nacimiento) y documentos (por número o rango de números de documentos denunciados)
  - Integración con Listas Negras Biométricas.

- Registro de Inspección de segundo nivel
  - Envío de registro de pasajero para supervisión.
  - Vista de alertas enviadas al Supervisor
  - Registro de la intervención del Supervisor mediante firma electrónica y la decisión considerada.
  - Interacción a través de mensajería entre Inspector y Supervisor.
  
- La solución permite que en cada Puesto Fronterizo se puedan utilizar los siguientes dispositivos, de acuerdo a las necesidades
  - Cámara para captura de Rostro e Iris
  - Scanner de Documentos de Viaje
  - Scanner para captura de Huellas Dactilares
  - Scanner para captura de Venas y Arterias
  - Scanner para documentación Extra
  - Impresora de Tickets
  
- La solución, a través de la integración de lectores de documento de viaje, incorpora los siguientes aspectos de seguridad, en la validación de la documentación presentada por el pasajero
  - Verificación cruzada de los datos de los Smart Chips
  - Verificación de información cruzada entre la MRZ y los datos del Smart Chip
  - Captura una gama completa de imágenes en color del documento usando fuentes de luz visible, infrarroja y ultravioletas, proporcionando un registro visual tanto de la información visible como de la leída mecánicamente.

## **BENEFICIOS**

Disponer de una Base de Datos con información digitalizada (demográfica y multibiométrica) de todas las personas que ingresan o egresan del País.

Agilizar los tiempos de atención en los puestos fronterizos, mediante la automatización en los procesos de registración.

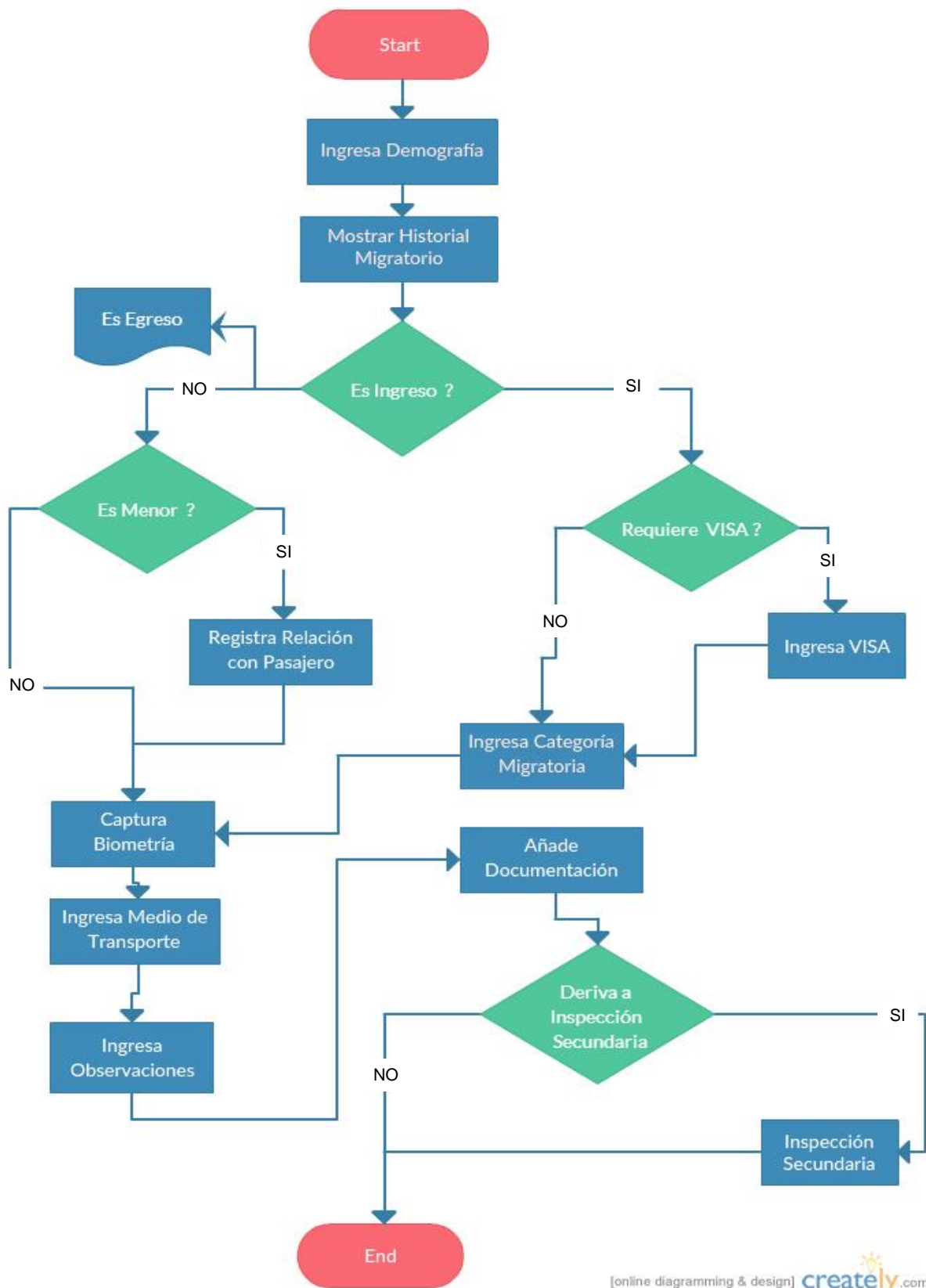
En caso que sea necesario, permite administrar una Black List (provista por organismos externos o no, por ejemplo Interpol, FBI, etc.) de personas buscadas por diferentes rasgos y seguir protocolos estandarizados en el momento del registro del pasajero.

Disponer de un nuevo sistema de control migratorio de última tecnología que permita la verificación de autenticidad de la documentación del viajero presentada (pasaporte y/o documento de viaje), a través de scanner especializados.

Disponer en los procesos de alta seguridad y valor agregado, cumpliendo con los estándares ICAO.

Permitir la obtención de estadísticas para los niveles de dirección que permitan verificar el volumen de trabajo y distribución por seccional para la concreción de mejoras en los servicios que se brindan a la comunidad.

## WORFLOW GENERAL DE LA INSPECCIÓN PRIMARIA



### **INSPECCIÓN PRIMARIA**

Será el puesto donde el pasajero entregará el documento de viaje, y demás documentación necesaria para el ingreso/egreso del país. En caso de existir algún inconveniente se enviará a la Inspección Secundaria.

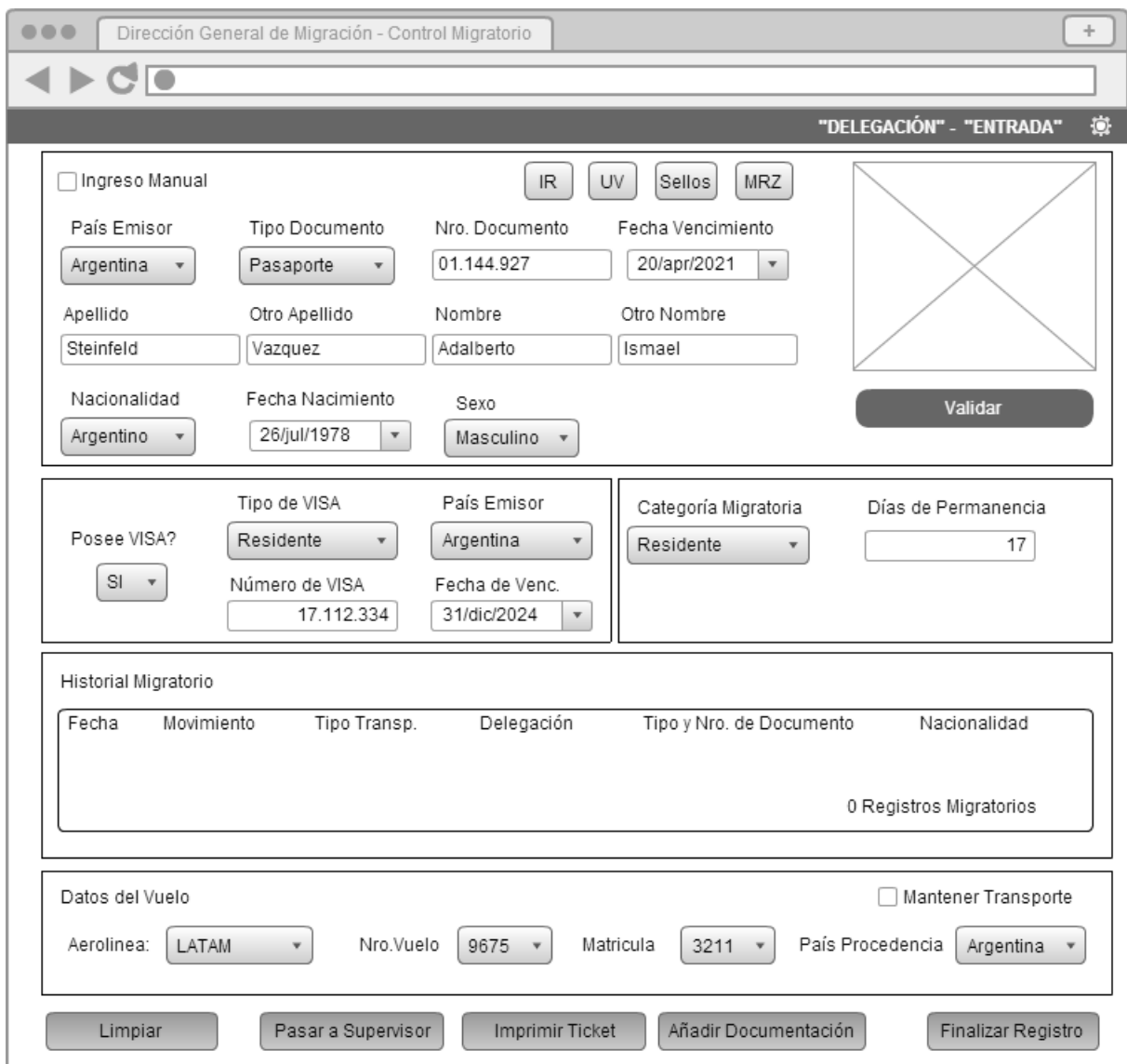
En la inspección primaria se efectuará las siguientes actividades:

- Escaneo de Pasaporte o Registro Manual
- Validación de Documentos
- Registro de Demografía
- Registro de Datos Biométricos
- Registro de Menores de Edad
- Registro de Visas
- Historial Migratorio
- Registro Ingreso/Egreso de Transporte Aéreo/Fluvial/Terrestre
- Registro de Datos Personales
- Escaneo de Documentación Adicional
- Notificaciones
- Emisión de Tickets
- Registro de Inspección de Movimiento Migratorio

El registro de la demografía de una persona puede realizarse de manera Manual o Automática, esta última, utilizando un Scanner de Documentos de Viaje. Cuando sea de manera Manual, será el usuario quien deba ingresar por teclado los datos demográficos.

El usuario deberá analizar si alguna de las personas mostradas en el historial de personas es la persona que está siendo registrada. Caso de ser así, se selecciona la persona correspondiente del listado, caso contrario la opción a seleccionar es “Una Persona Nueva”.

Para el registro de menores el sistema desplegará una nueva pantalla donde seleccionará el parentesco (Madre, Padre, Responsable) y mostrará todos los registros de inspección de egreso de la dependencia ingresados durante los últimos cinco minutos, en este listado permitirá seleccionar la persona mayor responsable para continua con el registro.



The screenshot shows a web browser window titled "Dirección General de Migración - Control Migratorio". The main content area is titled "DELEGACIÓN" - "ENTRADA". It contains several sections for data entry:

- Ingreso Manual:** Includes buttons for "IR", "UV", "Sellos", and "MRZ".
- Personal Data:**
  - País Emisor: Argentina
  - Tipo Documento: Pasaporte
  - Nro. Documento: 01.144.927
  - Fecha Vencimiento: 20/apr/2021
  - Apellido: Steinfeld
  - Otro Apellido: Vazquez
  - Nombre: Adalberto
  - Otro Nombre: Ismael
  - Nacionalidad: Argentino
  - Fecha Nacimiento: 26/jul/1978
  - Sexo: Masculino
- Visa Information:**
  - Posee VISA?: SI
  - Tipo de VISA: Residente
  - País Emisor: Argentina
  - Número de VISA: 17.112.334
  - Fecha de Venc.: 31/dic/2024
  - Categoría Migratoria: Residente
  - Días de Permanencia: 17
- Historial Migratorio:** A table with columns: Fecha, Movimiento, Tipo Transp., Delegación, Tipo y Nro. de Documento, Nacionalidad. It shows "0 Registros Migratorios".
- Datos del Vuelo:**
  - Aerolínea: LATAM
  - Nro. Vuelo: 9675
  - Matricula: 3211
  - País Procedencia: Argentina
  - Mantener Transporte:

At the bottom, there are buttons for "Limpiar", "Pasar a Supervisor", "Imprimir Ticket", "Añadir Documentación", and "Finalizar Registro".

### Registro Inspección Primaria – Ingreso

El sistema habilitará la posibilidad de registrar la Visa solo en caso que la nacionalidad y el tipo de documento de viaje con el que ingresa una persona lo requiera según la configuración establecida.

El Inspector puede enviar al Supervisor el registro de inspección en cualquier momento luego de capturar los datos demográficos de la persona.

El Inspector puede adjuntar documentación adicional a un registro de movimiento en cualquier momento luego del ingreso de los datos demográficos de la persona.

El usuario imprimirá el ticket cuando la persona que se encuentra en el registro de inspección no posea un documento donde asentar el movimiento migratorio.



Se considerarán los siguientes escenarios de excepción:

- Datos de Transporte Incompletos
- Datos de Visa incompletos
- Datos de Menor Incompletos
- Días de Permanencia Incorrectos
- Biometría Incompleta
- Deriva por Clones Encontrados
- Deriva por Coincidencia en Listas Negras
- Deriva por Verificación uno a uno
- Deriva por Datos Personales

El registro Biométrico estará compuesto por la Foto (que contemplará tanto Rostro como Iris) y las Huellas (que contemplará tanto dactilares como registro de venas), para el primero el sistema informará los indicadores de calidad de rostro luego de que la imagen fuera capturada (los indicadores ayudan a tomar acciones correctivas para re capturar fotografías con norma ICAO). Para la captura de Huellas el sistema informará aquellas con mala calidad para pedir que el usuario pueda re capturar en caso de ser requerido, al igual que con las venas. El sistema permitirá efectuar una cantidad limitada de re intentos de capturas antes de considerarla como un caso de Biometría Incompleta.



Pantalla Registro de Inspección – Captura Huellas y Venas Dactilares



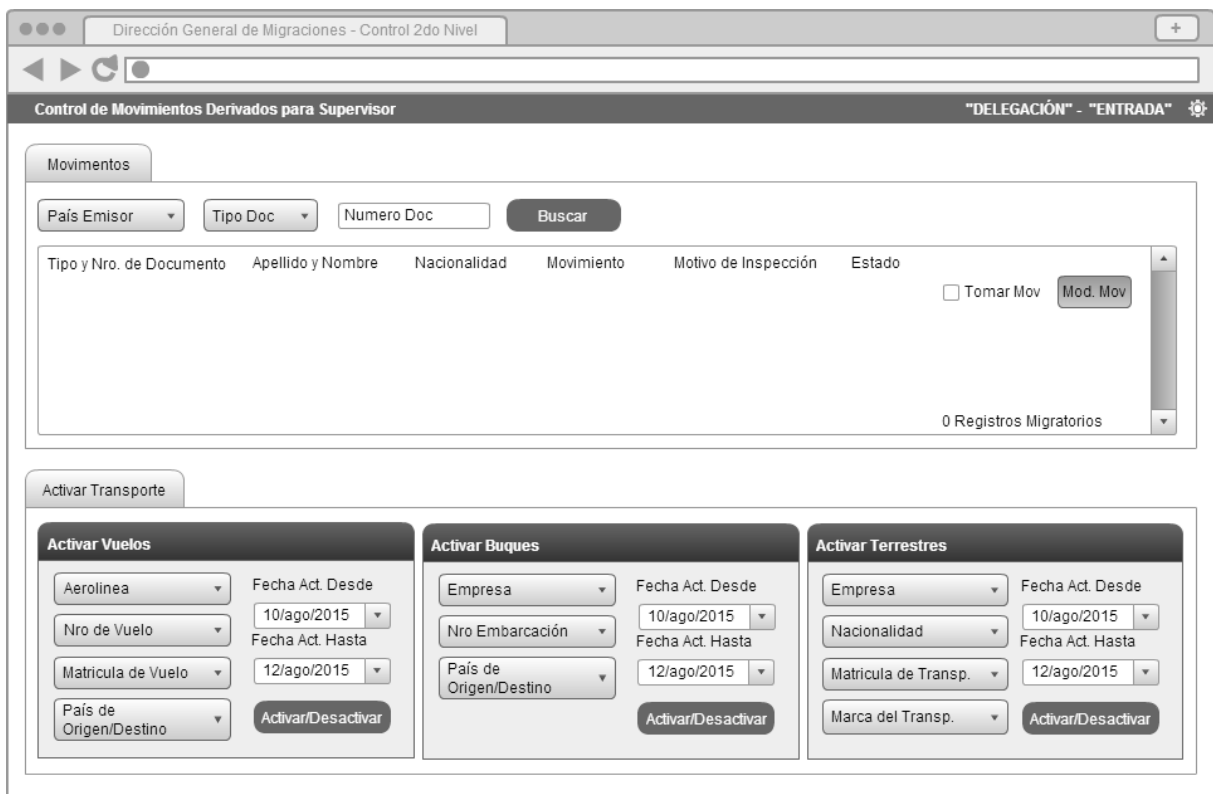
Pantalla Registro de Inspección – Captura Fotografía e Iris

## INSPECCIÓN SECUNDARIA

Permite evaluar un movimiento de pasajero proveniente de inspección primaria derivados a supervisión.

La inspección primaria es el primer paso en el movimiento migratorio de un pasajero, donde se registra el ingreso y egreso del mismo. La inspección secundaria es una instancia de análisis y control de un movimiento migratorio que contempla las siguientes acciones:

- Seleccionar Movimiento Pendiente de Análisis
- Buscar Movimiento por tipo y número de documento
- Activar o Desactivar Medios de Transportes ingresados nuevos
- Seleccionar y resolver un incidente registrado en el movimiento migratorio
- Modificar datos del movimiento migratorio derivado



The screenshot shows a web browser window titled 'Dirección General de Migraciones - Control 2do Nivel'. The main content area is titled 'Control de Movimientos Derivados para Supervisor' and includes a sub-header 'DELEGACIÓN - "ENTRADA"'. There are two main sections: 'Movimientos' and 'Activar Transporte'.

The 'Movimientos' section features a search form with fields for 'País Emisor', 'Tipo Doc', and 'Numero Doc', and a 'Buscar' button. Below the search form is a table with columns: 'Tipo y Nro. de Documento', 'Apellido y Nombre', 'Nacionalidad', 'Movimiento', 'Motivo de Inspección', and 'Estado'. A 'Tomar Mov' checkbox and a 'Mod. Mov' button are also present. The table currently shows '0 Registros Migratorios'.

The 'Activar Transporte' section contains three panels: 'Activar Vuelos', 'Activar Buques', and 'Activar Terrestres'. Each panel has several dropdown menus and date pickers for 'Fecha Act. Desde' and 'Fecha Act. Hasta', along with an 'Activar/Desactivar' button.

Registrar Inspección Secundaria – Movimientos y Activaciones

Para efectuar un veredicto el Supervisor de basa en el análisis de los Registros como Listas Negras, Detalles del Menor, Biometría Cruzada, Biometría Mal Capturada y/o Documentación Extra.

Esta función permite al Supervisor tomar un movimiento derivado del registro de inspección primaria a los efectos de poder ser analizado. El sistema permitirá al Supervisor consultar el detalle de los movimientos migratorios registrados por el Inspector a modo de contar con toda la información de respaldo para poder Aceptar o Rechazar el movimiento.

En la Activación o Desactivación de Medios de Transportes Ingresados nuevos, se corresponderá por las dependencias asignadas al usuario logueado, solo se podrán activar medios de transporte de la dependencia a la cual ha ingresado al sistema. Todo medio de transporte debe estar activado para ser utilizado en un registro de inspección primaria. Una dependencia puede ser configurada como Aérea, Fluvial o Terrestre.

La función de Desactivar Medios de Transporte permite la desactivación correspondiente a los medios de transportes registrados en la dependencia del usuario. Solo se puede ser desactivado los medios de transporte según el tipo de dependencia. Los procesos de desactivación son similares a los procesos descritos en la activación, solo que en este caso deberá contemplar que los transportes ya deben haber sido activados previamente.

La función de Modificar Movimiento Migratorio contempla la adecuación de los datos Demográficos, Datos de la Visa, Categoría Migratoria o Medio de Transporte.

Para Seleccionar un Incidente de Inspección cuya inspección fue aceptada pero por algún motivo el pasajero no pudiera entrar o salir del país, el Supervisor puede seleccionar un incidente para registrarlo en el movimiento indicando allí que ha sucedido un acontecimiento con la persona.

## ARQUITECTURA DEL SISTEMA INTEGRAL DE CONTROL MIGRATORIO

Arquitectura en Capas:

- Capa de base de Datos
  - Es la responsable del almacenamiento de datos.
  - Se accede a través de store procedure desde la capa de lógica de aplicación.
- Capa de Aplicación
  - Es la responsable de gestionar la lógica de negocio de toda la solución y de interactuar con la capa de datos
- Capa de Servicio Web
  - Es la capa que administra la interfaz web con la que interactuará el usuario.
- Puesto Cliente conectados a través de un browser a la capa WEB
- La solución permite la integración con otros sistemas, esa integración y es controlada a través de la capa lógica de negocio o web, dependiendo del modo de interconexión.



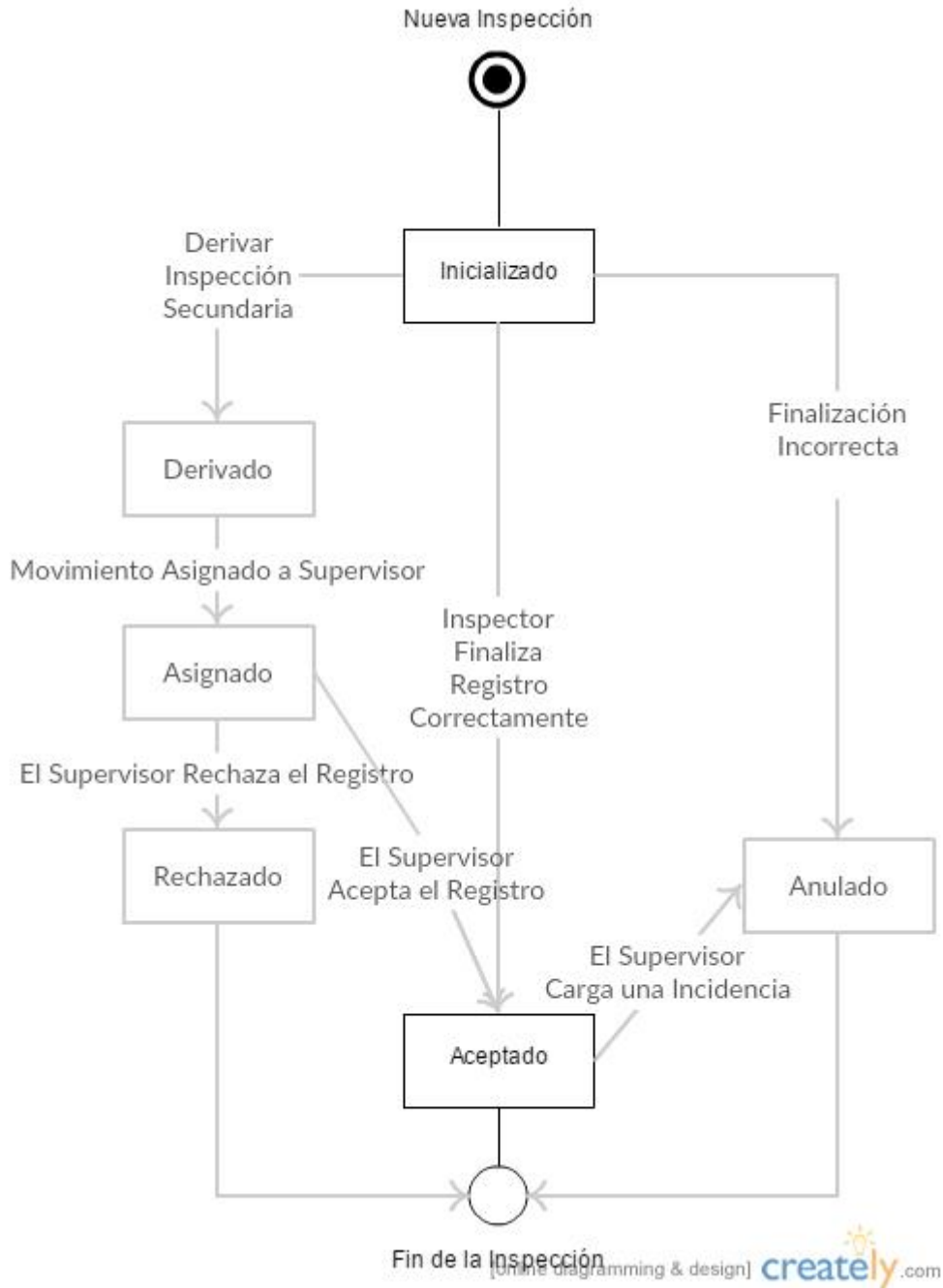
Mediante el complemento de Administración de la Base Única, se administrarán los nomencladores necesarios para las diferentes categorías contempladas dentro del sistema como por Ejemplo Marcas de Vehículos, Categorías Migratorias, Países, Provincias, Estados, Municipios, Tipos de Documentos, Etc.

También se podrá efectuar la administración de Usuarios permitiéndolos vincular con el sistema, tanto usuarios internos como externos siempre que estén registrados y efectuadas las correspondientes validaciones. El proceso permitirá asociar una Persona a un Usuario del sistema.

## MODELO DE NEGOCIO

### a) Identificación de los estados

El presente diagrama muestra los estados de un registro de inspección y sus transiciones.



### b) Identificación de los casos del negocio

- Rol del Administrador

- Rol del Inspector
- Rol del Supervisor

Rol Inspector	Rol Administrador	Rol Supervisor
Añadir Documentación Entrada Aérea Entrada Fluvial Entrada Terrestre Registrar Biometría Registrar Menor con Acompañante Registrar Menor sin Acompañante Salida Aérea Salida Fluvial Salida Terrestre	Administrar Transportes Aéreos Administrar Transportes Fluviales Administrar Transportes Terrestres Agregar Dependencias Asociar Empleados a Dependencias Buscar Dependencias Configurar días de Permanencia Configurar Reglas de Edades Configurar Visas Gestionar Lista Negra de Documentos Gestionar Lista Negra de Personas	Listado de Movimientos Pendientes Supervisar Entrada Supervisar Salida Ver Detalle de Movimiento
		Login
		Login Seleccionar Aplicativo/Rol/Ambiente Seleccionar Dependencia Seleccionar Modalidad de Trabajo

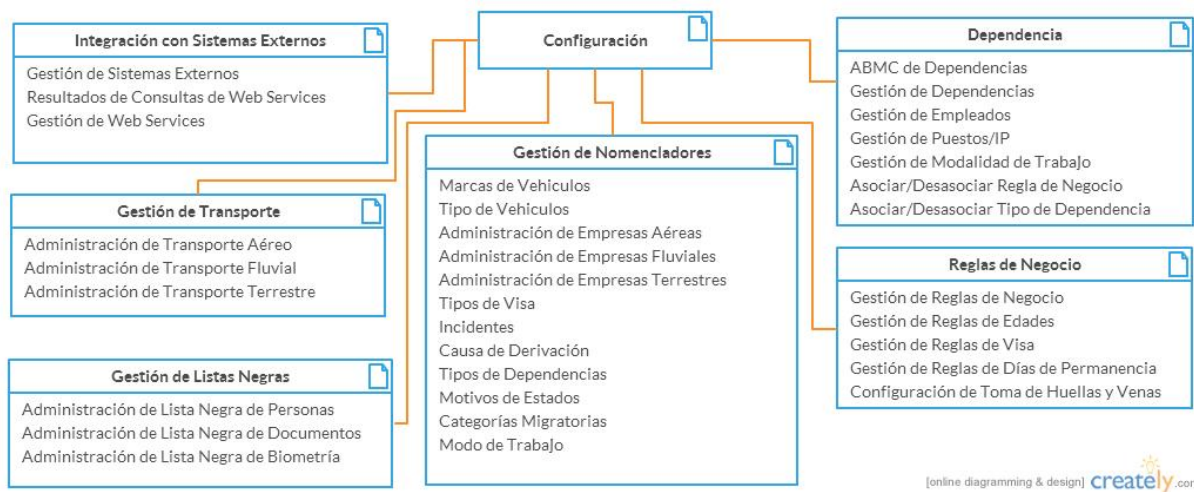
**c) Propuesta Funcional**

- Rol del Administrador contemplará los casos desarrollados de Configuración
- Rol del Inspector contemplará los casos desarrollados de Inspección Primaria
- Rol del Supervisor contemplará los casos desarrollados de Inspección Secundaria

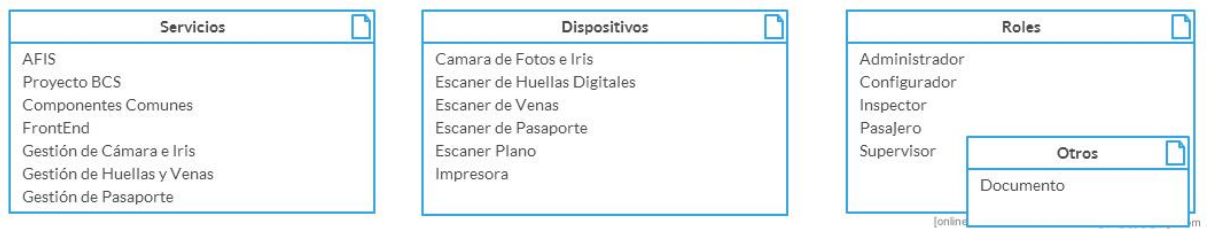
Login	Configuración	Inspección Primaria
Seleccionar Dependencia de Trabajo Seleccionar Modalidad de Trabajo	Administrar Transporte Aéreo Administrar Transporte Fluvial Administrar Transporte Terrestre Administrar Dependencias Asociar Empleado a Dependencia Asociar Puesto a Dependencia Configurar Listas Negras de Documentos Configurar Lista Negra de Personas Configurar Lista Negra de Datos Biométricos Configurar Días de Permanencia Configurar Reglas de Visa Configurar Rangos de Edades Configurar Toma de Huellas y Venas	Confirmar Persona Completa Información para Menores Escanea Datos Biométricos Escanea Documentación Derivar Persona a Supervisión
Reportes		Inspección Secundaria
Cantidad de Ingresos Cantidad de Egresos Movimientos de Pasajeros Inspección Primaria Inspección Secundaria Positivos contra Listas Negras		Biometría Cruzada Alertas de Cruce contra Listas Negras Modifica Datos Movimiento Define Incidencia



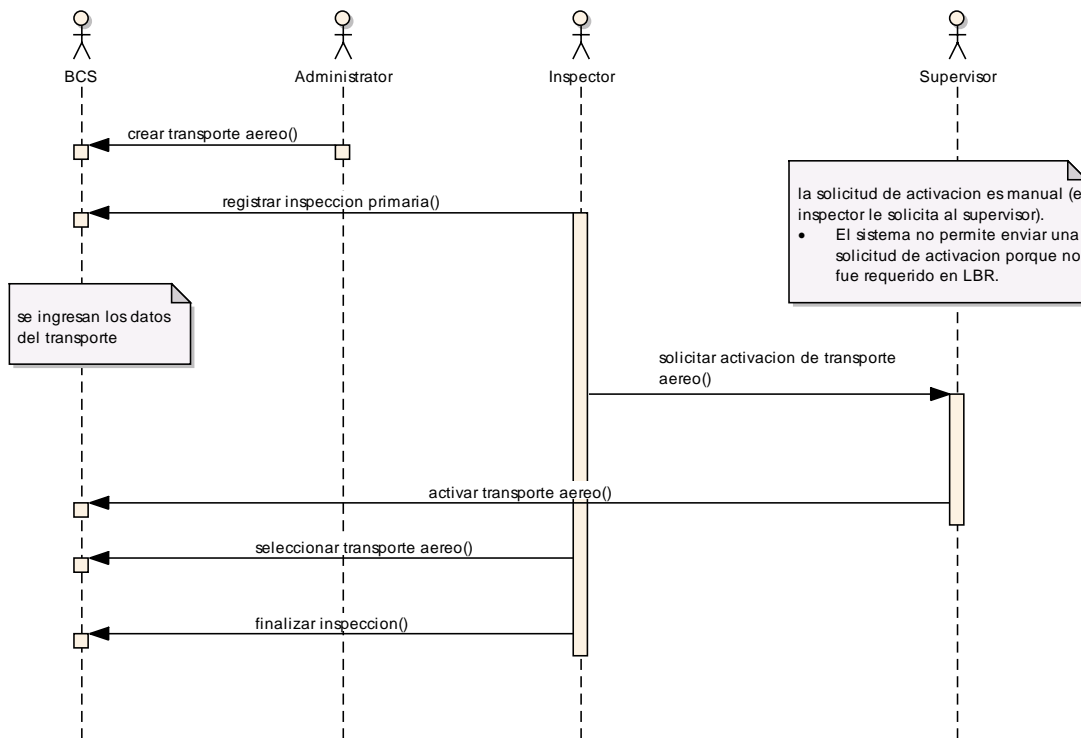
## REQUERIMIENTO DE CONFIGURACIÓN:



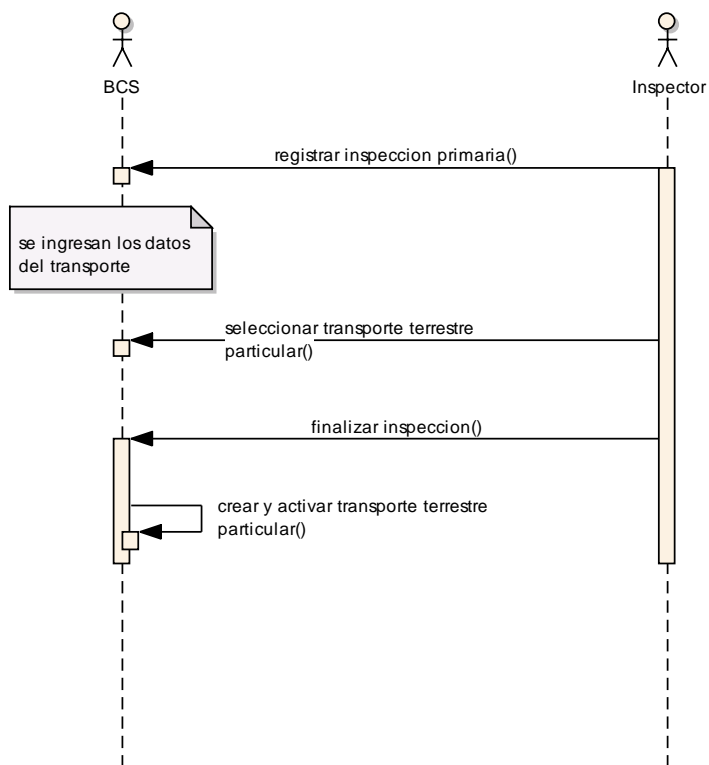
## ACTORES



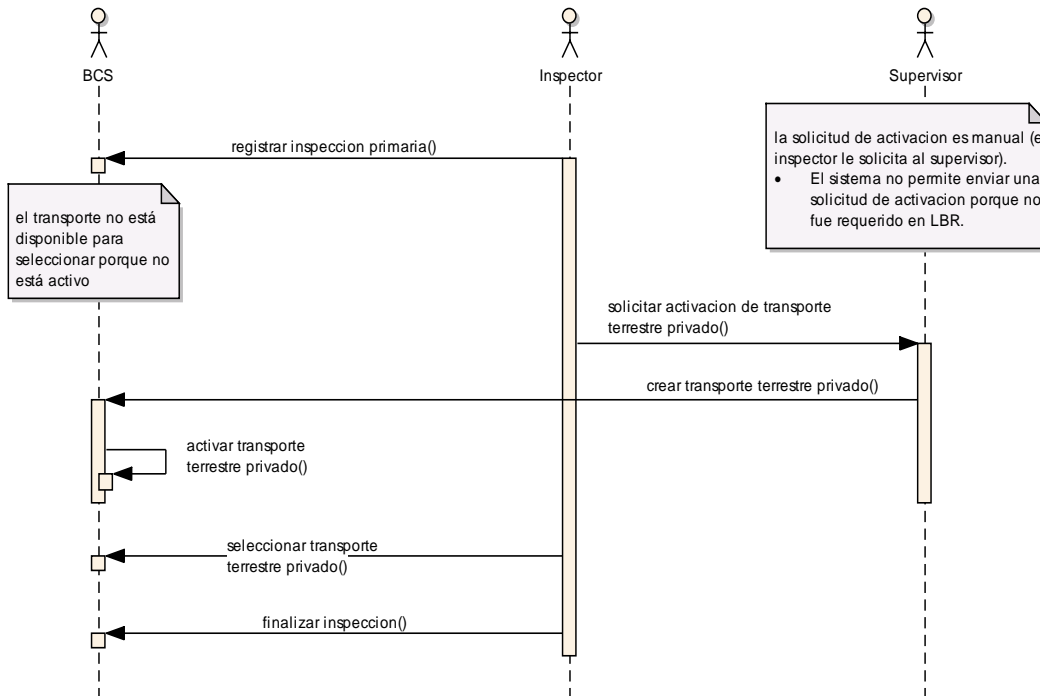
*Crear y Activar Transporte Aéreo y Fluvial*



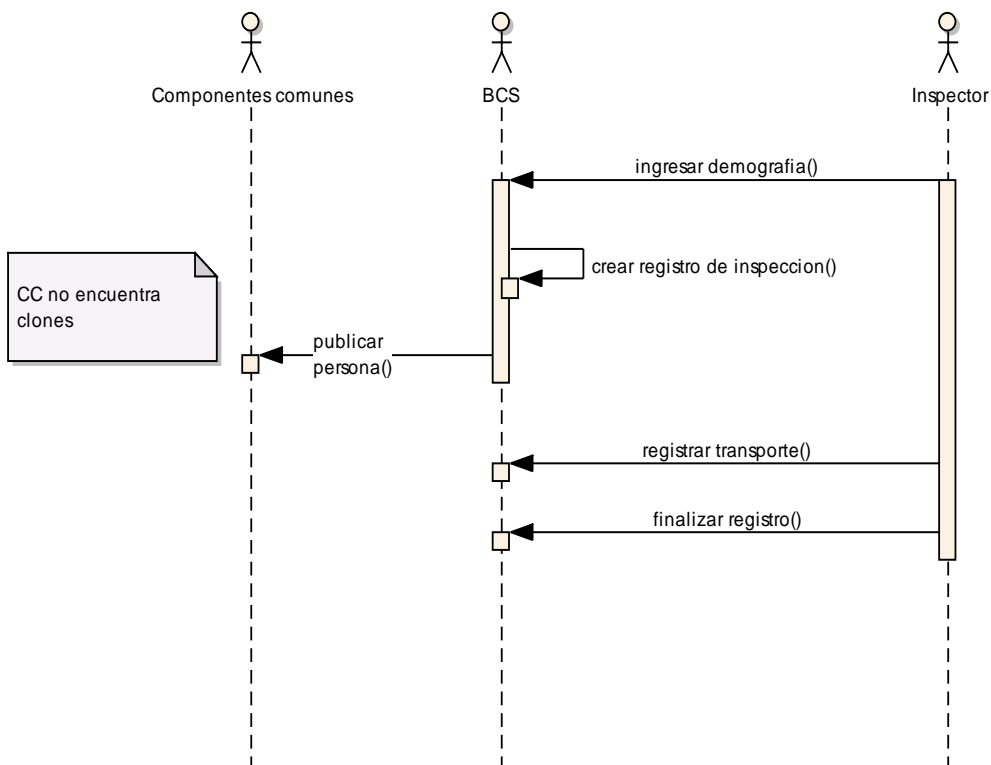
Crear y Activar Transporte Terrestre Particular



### Crear y Activar Transporte Terrestre Privado

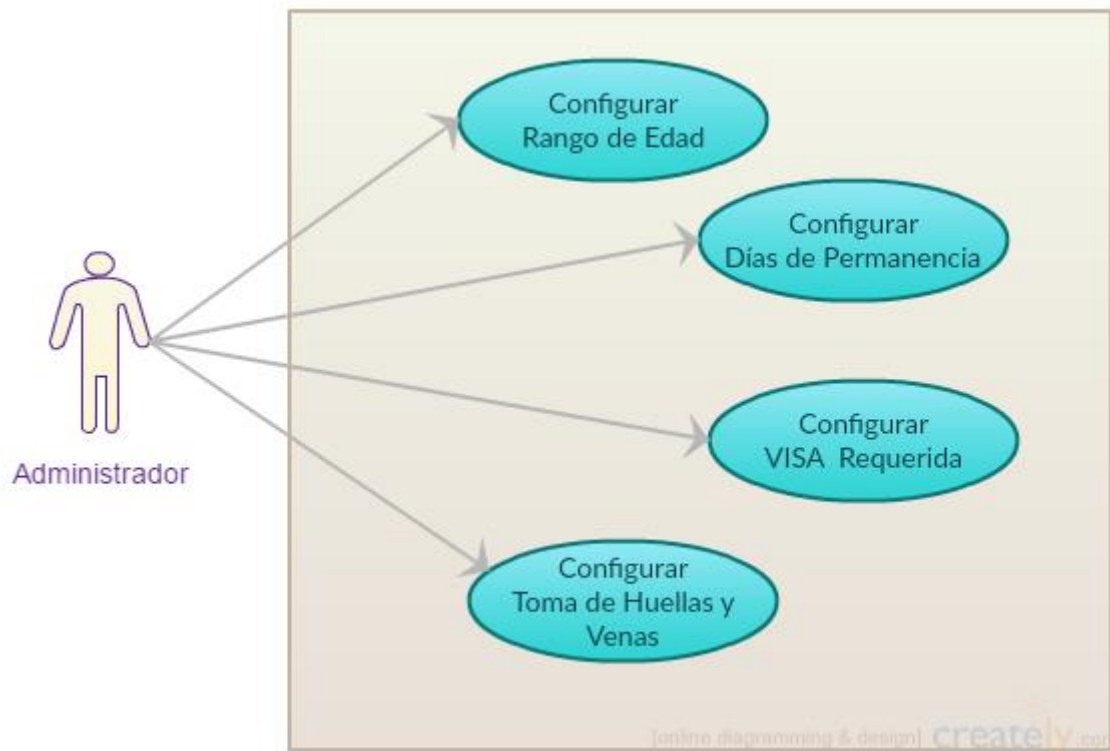


**Registrar Inspección Primaria de Pasajero (Carga Manual sin Dispositivos)**



## CASOS DE USO

### CU: Reglas de Negocio



#### Configurar Rango de Edad

Se debe configurar en el sistema hasta que edad un menor deber salir acompañado con un adulto, independientemente de las autorizaciones judiciales de los padres.

En caso de que no aplique esto para un determinado país, el valor a configurar debe ser -1

- El sistema manejará rangos de menores, las cuales deberán ser configurables.

Para el ejemplo del caso de Argentina el rango es de 0 a 7 y de 8 a 17.

- Si el menor se encuentra dentro del primer rango es obligatorio que este acompañado por los dos padres, uno de ellos, un tutor o responsable. En caso de que no estén los dos padres presentes en el movimiento migratorio se deberá registrar la Orden del Juzgado.
- Si el menor se encuentra dentro del segundo rango podrá salir sin ser acompañado por ningún mayor, pero será necesario y obligatorio poseer el permiso.
- Hay que contemplar el caso de que el menor de edad, de 7 a 18, se encuentre emancipado, en ese caso no será necesario ninguna orden de juzgado.

### Configurar Días de Permanencia

Las categorías de ingreso (no residente / residentes) tiene la siguiente información:

- Categoría Migratoria
- Código País
- Código Subcategoría migratoria (Numérico,5)\* Proviene del ABMC Categoría Migratoria
- Cantidad días permanencia (int) (indica cuántos días puede estar en el país la persona)
- Fecha de Vigencia Desde / Hasta
- Check de activación.

\* Todos los campos son de carácter obligatorio, en caso de no tener límite de día se pone -1.

Cada categoría de ingreso deberá tener un máximo de días de permanencia, los cuales deberán darse de alta en esta regla de negocio.

### Configurar Visa Requerida

Según la Nacionalidad y el tipo de documento de viaje con que ingresa una persona, se determina si requiere Visa, por lo tanto se debe configurar en el sistema:

- Nacionalidad (desplegable) ( Proviene desde Nomencladores)
- Tipo de documento (desplegable)
- Categoría de Visa (desplegable) se obtiene de Componentes Comunes (requiere/no requiere / consultada)
- Activa (si/no) \*
- Fecha desde (fecha)\*
- Fecha hasta (fecha) (puede estar vacía)

\* Estos campos permiten soportar que un país requiere Visa en un periodo, y dejen de requerirlo, o viceversa.

Se debe controlar que para un mismo país y tipo de documento, no existan periodos superpuestos.

Se deberá tener en cuenta reglas especiales que se acuerdan con cada país. Por ejemplo para el caso planteado, si el pasajero proviene de la República Popular de China y en su pasaporte se lee "Nationality British Citizen" se le dará tratamiento de 'Exento de Visa', caso contrario se dará tratamiento como 'Visa Consultada (C)'.

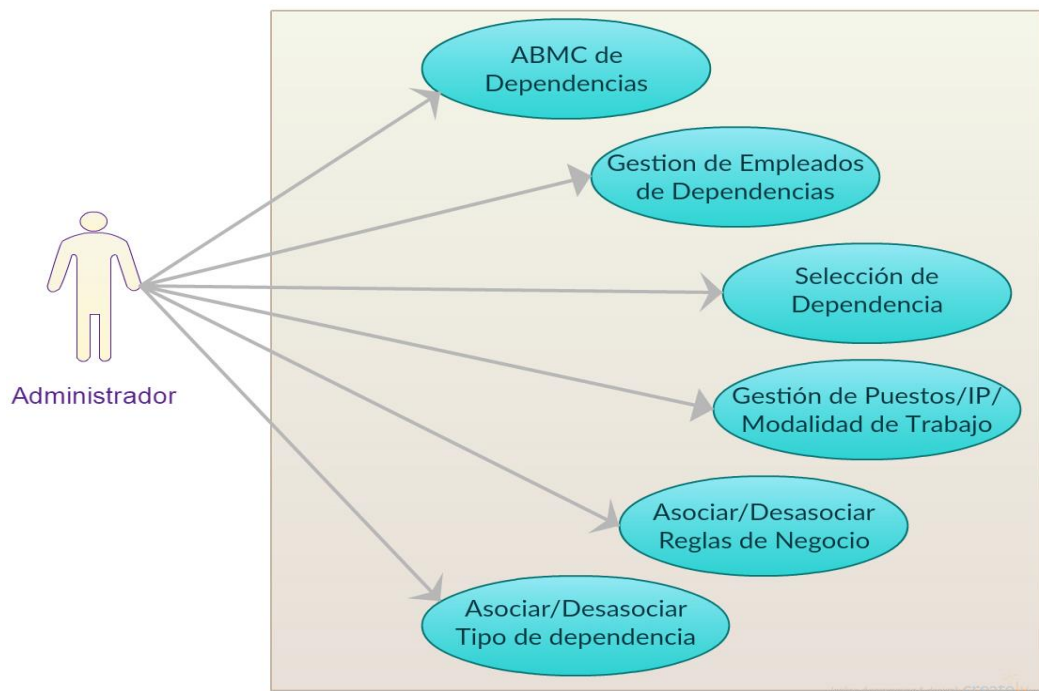
### Configuración Toma de Huellas y Venas

Se deberá poder configurar la toma de huellas dactilares. Esto refiere a que si el pasajero ya posee movimientos migratorios se deberá poder configurar (dependiendo cada país) la toma de las huellas. Siendo 4-4-2 la primera vez y luego solamente 4 o 2.

- En caso de configurar 2, serán los pulgares
- En caso de configurar 4, será el meñique, anular, medio e índice de la mano derecha.
- En caso de configurar Mano Izquierda solamente
- En caso de configurar Ambas Manos.



CU: Gestión de Dependencias



**ABMC Dependencias**

Será un Alta/Baja/Modificación/Consulta de dependencias.

Se darán de alta todas las Dependencias y en los marítimos y terrestres se detallarán con el país que limita, siempre que sea 1 a 1. Ej.: Caso puerto de Bs As limita con todos los países por ende no se detalla el país que limita se dejaría un valor -1 para que se muestren todos los países cuando se active algún buque.

Los datos a ingresar son:

- Código (Numérico, 255)\*
- Tipo de Dependencia (Numérico, 5)\* Proviene del ABM de Tipo de Dependencia
- Nombre de Dependencia (Numérico, 255)\*
- Ubicación: (País, Provincia, Localidad, Dirección)\* Proviene de Componentes Comunes
- Rango IP: desde-hasta (No puede existir dos rango iguales)
- Limita? (SI/NO)\* en caso de ser SI el código país es obligatorio, caso contrario automáticamente se pondrá -1 en código país.
- País (Numérico, 255) \* Desplegable. Proviene de País de Componentes Comunes.

\* Todos los campos son de carácter obligatorio.

### Gestión de Empleados de Dependencias

Se debe permitir asociar a un usuario de base única (nombre de usuario) a una o más Dependencias, así como desasociar una que ya tenga configurada.

Cuando se selecciona un usuario, se mostrarán las delegaciones asociadas, y el usuario podrá asociar una adicional, o desasociar una de las mostradas.

### Selección de Dependencia

Cuando el usuario acceda por medio del control de acceso, el sistema realizará las validaciones correspondientes, validando si el usuario es Supervisor o Inspector.

En caso de que sea Supervisor el Sistema mostrara la pantalla asociada a la Dependencia en la cual esta logueado físicamente, es decir que la dependencia será inferida a través de la IP del puesto.

En caso de que sea Inspector, el sistema validara la modalidad de trabajo del puesto donde se está realizando la firma, y dependiendo el Medio de transporte asociado a la dependencia mostrará la pantalla correspondiente.

En caso de que la modalidad de trabajo sea Entrada/Salida, el Inspector seleccionara la opción con la cual desea trabajar, pudiendo cambiar la modalidad una vez logueado desde el menú, y el sistema lo llevara la opción seleccionada.

### Gestión de Puestos/IP/Modalidad de Trabajo

Se deberá configurar cada puesto de trabajo de la Dependencia, al mismo se le deberá asociar:

- IP → Cada Dependencia deberá tener un rango de IP.
- Modalidad de Trabajo → Las posibles modalidades de trabajo de un puesto serán: Entrada, Salida y Entrada/Salida.

La asignación de modalidad de trabajo es a nivel puesto pero el sistema debe permitir asignar una modalidad de trabajo a muchos puestos de trabajo de una dependencia.

### **Asociar/Desasociar Reglas de Negocio**

A cada Puesto se le podrá asociar o desasociar, según sea el caso, la/s regla/s de negocio/s que corresponda o aplique en cada caso.

La asignación de reglas es a nivel puesto pero el sistema debe permitir asignar muchas reglas a muchos puestos de trabajo de una dependencia.

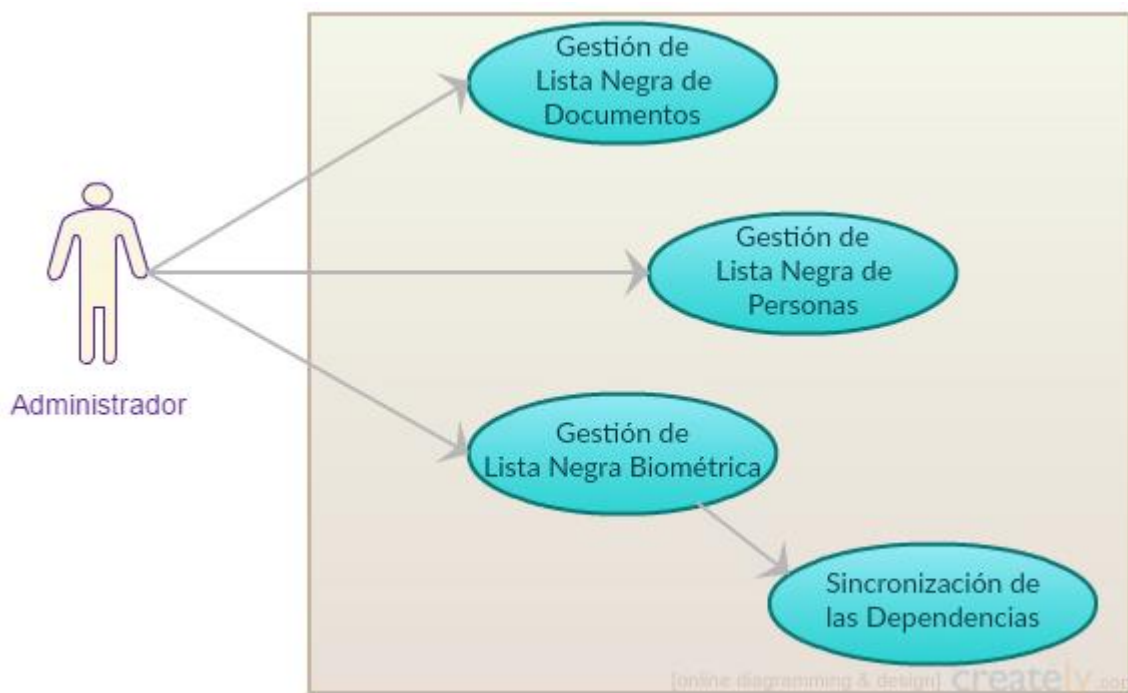
### **Asociar/Desasociar Tipo de dependencia**

Se tomaran los datos del Nomenclador correspondiente a Transportes, los valores serán:

- Aéreo
- Marítimo
- Terrestre

A cada dependencia se le deberá asociar UN UNICO tipo de paso fronterizo.

**CU: Gestión de Listas Negras**



**Gestión de Lista Negra de Documentos**

Se registran los números de documentos de viaje que están dentro de la Black List:

- País Emisor \* (proviene de Componentes Comunes)
- Tipo de Documento (desplegable): \* (El tipo de documento viene desde Componentes Comunes)
- Número de Documento (Numérico) ej. AAR678U - TYU789 \*

\*Son los campos obligatorios

**Gestión de Lista Negra de Personas**

Se administra la Black List de personas por su nombre y fecha de nacimiento:

- Nombre (texto)\*
- Apellido (texto)\*
- Fecha de Nacimiento (fecha)

\*Son los campos obligatorios

### Gestión de Lista Negra Biométrica

En caso de disponer de información para la Black List biométrica, se dispondrá de un AFIS en dónde estén registradas las huellas de las personas dentro de la Black List, por lo tanto, cuando se registran las huellas de una persona, se realizará una búsqueda 1:N contra la Black List del AFIS.

### Sincronización de las Dependencias

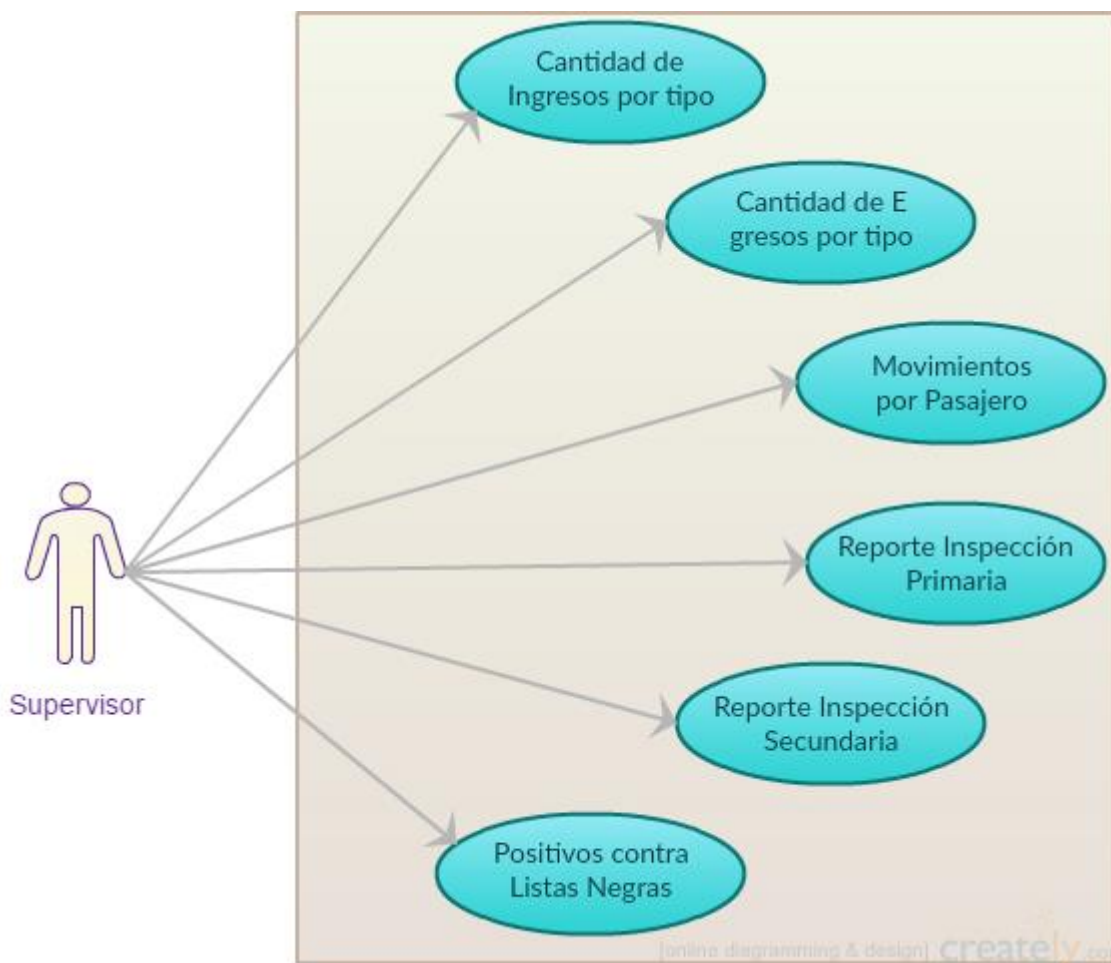
El Sistema de Control Migratorio deberá tener un mecanismo de sincronización para trabajar en un esquema en donde todas o algunas Delegaciones trabajen en forma local, sincronizando contra el Sistema Central.

- En el Sitio Central deberán de darse de alta todos los usuarios con sus roles y a qué dependencias pertenece. Sincronización desde el Sitio Central hacia las Dependencias
- Cada Dependencia administrará sus usuarios, por ejemplo cambio de puesto.
- El Sitio Central administrará los nomencladores, las Business Rules y la Black List (por Nro. Documento y Personas) y Dependencias. Todo esto se sincroniza desde el sitio central hacia cada Dependencia (Nodo)
- Todo movimiento registrado en cada dependencia (Entrada/Salida) se sincronizará contra el Sitio Central.
- El sistema deberá operar de la misma forma, ya sea en una Delegación local, que en manera centralizada, exceptuando los siguientes casos:

Si existe un chequeo contra Black List de biométrica, y localmente no dispone de un AFIS de Black List, este paso no será efectuado en el momento. Se chequeará en el momento de sincronizar, y solo enviará un aviso a los supervisores para que comuniquen a alguna entidad que justifica. (Configurable, podría ser por mail enviando los datos del hit). En caso de dar aviso al Supervisor, se le enviara un mail con los datos de la persona que dio Hit contra Black List.

- No dispondrá de integración contra ningún sistema que esté disponible solo en el sistema central.

CU: Gestión de Reportes



**Cantidad de Ingresos Por Tipo**

Se deberán poder consultar un listado de ingresos por día, según el siguiente filtro:

- Fecha desde
- Hora desde
- Fecha hasta
- Hora Hasta
- Tipo de Transporte: permitir seleccionar todos, uno, o algunos. (proviene de ABM tipo de transporte)
- Dependencia: permitir seleccionar todos, uno, o algunos. Proviene de ABM dependencia.

Se deberá mostrar en el listado:

- Fecha y hora del movimiento

- Datos del pasajero (nombre y nro. de documento)
- País de Origen
- Tipo de Transporte
- Detalle del medio de transporte, según el tipo. \*1
- Dependencia: proviene de ABM dependencias.
- Observaciones: si corresponde (mostrar observaciones ingresadas por el Inspector)

\*1 Si es aéreo se mostrara compañía (código IATA) y numero de vuelo.

- Si es fluvial se mostrara la compañía fluvial, la matricula del barco y el código OMI
- Si es terrestre (de empresa de micros) se mostrara el nombre de la compañía.
- Si es terrestre (particular) se mostrar la patente y la marca del vehículo

<b>Cantidad de Egresos Por Tipo</b>
-------------------------------------

Se deberán poder consultar un listado de egresos por día, según el siguiente filtro:

- Fecha desde
- Hora desde
- Fecha hasta
- Hora Hasta
- Tipo de Transporte (todos, uno, o algunos) (proviene del ABM Tipo de Transporte)
- Dependencia (todas, una o algunas)

Se deberá mostrar en el listado:

- Fecha de Egreso
- Datos del pasajero (nombre y nro. de documento)
- País de Destino
- Tipo de Transporte
- Detalle del Tipo de transporte, según el tipo \*1
- Delegación
- Observaciones si corresponde

\*1 Si es aéreo se mostrara compañía (código IATA) y numero de vuelo.

- Si es fluvial se mostrara el compañía fluvial, la matricula del barco y el código OMI
- Si es terrestre (de empresa de micros) se mostrara el nombre de la compañía.
- Si es terrestre (particular) se mostrar la patente y la marca del vehículo

## Movimientos por Pasajero

A partir de los datos de un pasajero, se deberán mostrar todos los movimientos migratorios registrados para el mismo.

Filtros de búsqueda del pasajero por:

- Nombres
- Apellidos
- Fecha de Nacimiento
- Tipo y número de Documento

Datos a mostrar:

- Fecha de registro
- Tipo (ingreso / egreso)
- País de Origen/Destino
- Tipo de Transporte: (Proviene del ABM Tipo de Transporte)
- Datos Visa (si corresponde): (Nro. Visa)
- Observaciones: (Cualquier observación que haya sido ingresada en la inspección)

## Reporte Inspección Primaria

Se podrá obtener un reporte según el puesto de inspección primaria seleccionando el siguiente filtro:

Filtros de búsqueda del pasajero por:

- Dependencia
- Tipo de Movimiento (seleccionará Ingreso, Egreso o ambos)
- Fecha desde
- Fecha Hasta (por default deberá mostrar la sysdate)

Deberá mostrar:

- Dependencia
- Fecha de Inspección
- Nombre completo del Inspector
- Puesto/Movimiento (Ingreso o Egreso, según se haya seleccionado en el filtro)
- Nombre y Apellido (del pasajero)
- Nro. Documento
- País Origen / País Destino (según corresponda el movimiento seleccionado).



- Chequeo con Black List (en caso de que no haya podido realizar control contra Black List por vínculo caído mostrará un NO, caso contrario SI)
- Total de registros (El sistema deberá mostrar el total de registros que se muestran)

\*Las Columnas 'Nombre Completo del Inspector' y 'Puesto/Movimiento' deberán poder seleccionarse para ordenar según se requiera.

### **Reporte Inspección Secundaria**

Se podrá obtener un reporte según el puesto de inspección secundaria seleccionando el siguiente filtro:

- Dependencia
- Tipo de Movimiento (seleccionará Ingreso o Egreso)
- Fecha desde
- Fecha Hasta (por default deberá mostrar la sysdate)

Deberá mostrar:

- Dependencia
- Fecha Inspección
- Nombre completo del Supervisor
- Movimiento (Ingreso o Egreso, según se haya seleccionado)
- Nombre y Apellido (del pasajero)
- Nro. Documento
- País Origen / País Destino (según corresponda el movimiento seleccionado).
- Causa de Supervisión
- Comentario
- Nombre Completo del Inspector
- Resultado de Supervisión

\*Las Columnas 'Nombre Completo del Supervisor', 'Causa de supervisión' y 'Resultado de Supervisión' deberán poder seleccionarse para ordenar según se requiera.

**Positivos contra Listas Negras**

Se podrá obtener un reporte por los casos que dieron positivo en el control contra la Black List, seleccionando el siguiente filtro:

- Dependencia: listado de dependencias pudiendo seleccionar uno o muchos.
- Tipo de Movimiento (seleccionará Ingreso o Egreso)
- Fecha desde: (Fecha de registro)
- Fecha Hasta (por default deberá mostrar la sysdate)

Deberá mostrar:

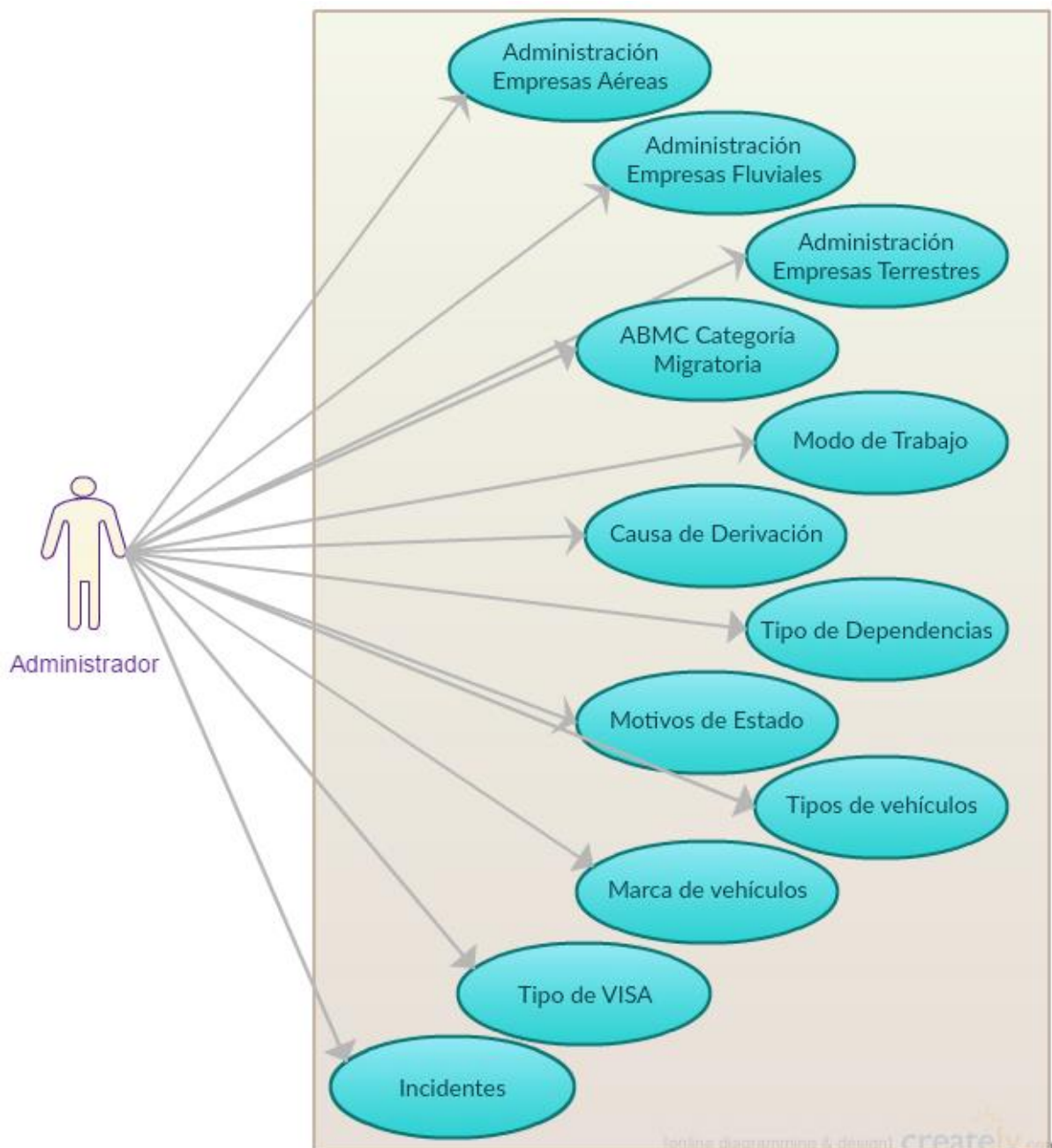
- Movimiento (Ingreso o Egreso, según se haya seleccionado)
- Nombre y Apellido (del pasajero)
- Nro. Documento
- País Origen / País Destino (según corresponda el movimiento seleccionado).
- Causa de Supervisión: )Proviene del ABMC de Causas)
- Nombre completo del Supervisor:
- Comentario: comentario 2da nivel según pantalla 002.2? (SI)
- Nombre Completo del Inspector
- Resultado de Supervisión: (Ingreso o Rechazo)

\*Las Columnas 'Nombre Completo del Supervisor', 'Causa de supervisión' y 'Resultado de Supervisión' deberán poder seleccionarse para ordenar según se requiera.

**CU: Gestión de Nomencladores**

El sistema permite la gestión de nomencladores para la configuración del sistema.

Los nomencladores que aquí se definen deben ser creados desde SABU, siendo consumidos por la vertical de Control Migratorio.



### Administración Empresas Aéreas

Aquí se darán de alta las empresas que actuaran en los pasos fronterizos (dependencias), ejemplo:

Aéreo: LAN, Aerolíneas Argentina, British Airways, etc.

Se debe ingresar:

- Código (Numérico, 10) \* (código IATA que es un código internacional OACI)
- Nombre de la compañía. (Alfanumérica, 100) \*

\*Son los campos obligatorios

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá cargar esta funcionalidad

Tener en cuenta que existen vuelos privados (PRV) y vuelos especiales (ESP). Los ESP son vuelos que las aerolíneas ponen para el traslado por ejemplo del seleccionado argentino de futbol, en ese caso la aerolínea declara que hará ese vuelo especial denunciando el número de vuelo. Los privados si se programan con anterioridad se darán el mismo trato, caso contrario se cargara el PRV en el día y se activara posteriormente.

### Administración Empresas Fluviales

Aquí se darán de alta las empresas que actuaran en los pasos fronterizos, por ejemplo:

Se debe ingresar:

- Código (Numérico, 10) \*
- Nombre compañía. (Numérico, longitud 100) \* Se deberá poder dar de alta la de la compañía PRV, descripción Privado, para tratamiento de vehículos particulares

\*Son los campos obligatorios

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá cargar esta funcionalidad

### Administración Empresas Terrestres

Aquí se darán de alta las empresas que actuaran en los pasos fronterizos, por ejemplo:

- Terrestre: Chevallier, Empresa Argentina, etc.

Se debe ingresar:

- Código (Numérico, 10) \* Se deberán mostrar los códigos de las empresas, x ejemplo Crucero del Norte CDN, este último valor será el que se mostrará en el combo de empresa en el paso fronterizo terrestre.
- Nombre de la compañía. (Alfanumérica, 100) \* Se deberá poder dar de alta la de la compañía PRV, descripción Privado, para tratamiento de vehículos particulares
- Nacionalidad. (Se mostrara la descripción y proviene del Nomenclador País) En el caso de días PRV (Particulares) este campo se completara según lo que se ingrese en la Activación.

\*Son los campos obligatorios

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá cargar esta funcionalidad

### ABMC Categoría Migratoria

Las categorías migratorias (residente / no residente) tienen la siguiente información:

- Código (Numérico, 10)
- Nombre (Numérico, 100)

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá cargar esta funcionalidad

#### Residentes

Se deberá detallar en esta categoría de Residentes:

- Código (Numérico, 10)
- Nombre (Numérico, 100)
  - Por Ejemplo: Residentes Temporales; Residentes Permanentes

### No Residentes

Se deberán de dar de alta para esta categoría de No Residentes:

- Código (Numérico, 10)
- Nombre (Numérico, 100)
  - Por Ejemplo: Personas en Tránsito; Turistas y/o visitantes.

<b>Modo de Trabajo</b>
------------------------

Se debe de dar de alta la modalidad de trabajo, las opciones son:

- Entrada
- Salida
- Entrada/Salida

Se debe ingresar:

- Código (Numérico, 10)
- Nombre (Numérico, 100)

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá cargar esta funcionalidad

<b>Causa de Derivación</b>
----------------------------

Se darán de alta las causas por las que un pasajero es pasado a inspección secundaria.

Se deberán ingresar los siguientes datos:

- Código (Numérico, 10)
- Descripción (Numérico, 100)

Incidencia toma biométrica por mala calidad

- Documento inutilizable
- Black List Personas
- Black List Documento
- Black List Biométrica
- No cumple condición migratoria

### Tipo de Dependencias

Es un ABMC del tipo de Dependencias existentes:

- Aéreo
- Marítimo
- Terrestre

Los valores a ingresar son:

- Código (Numérico, 10)\*
- Descripción (Numérico, 100)\*

\*Todos los campos son de carácter obligatorios.

### Motivos de Estado

Es un ABMC de los motivos por los cuales el movimiento de un pasajero pasa por los estados disponibles para el proceso de migraciones.

Los campos a ingresar son:

- Código (Numérico, 10)\*
- Descripción (Numérico, 100)\*

\* Todos los campos son de carácter obligatorio.

### Tipos de vehículos

Se darán de alta los tipos de vehículos.

Se debe ingresar:

- Código (Numérico, 10)
- Tipo vehículo (Numérico, longitud 100)
  - Por Ejemplo: Auto, Micro, Combi, camioneta, Camión, Camión c/Acoplado)

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá utilizar esta funcionalidad.

- Este requerimiento es un ABMC y no requiere integración con otros sistemas.

**Marca de vehículos**

Se darán de alta las empresas de vehículos.

Se debe ingresar:

- Código (Numérico, 10) \*
- Nombre de Marca de vehículo (Numérico, longitud 100) \*

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá utilizar esta funcionalidad.

Este requerimiento es un ABMC y no requiere integración con otros sistemas.

**Tipo de Visa**

Se configurara aquí los tipos de Visa que sean requeridas para el país.

Lo datos a cargar son:

- Código (Numérico, 10) \*
- Nombre (Numérico, 100)\*
  - Por Ejemplo: SIN Visa; Visa CONSULAR o Visa CONSULTADA

**Incidentes**

El presente nomenclador será utilizado al momento de modificar el estado de un movimiento ya registrado.

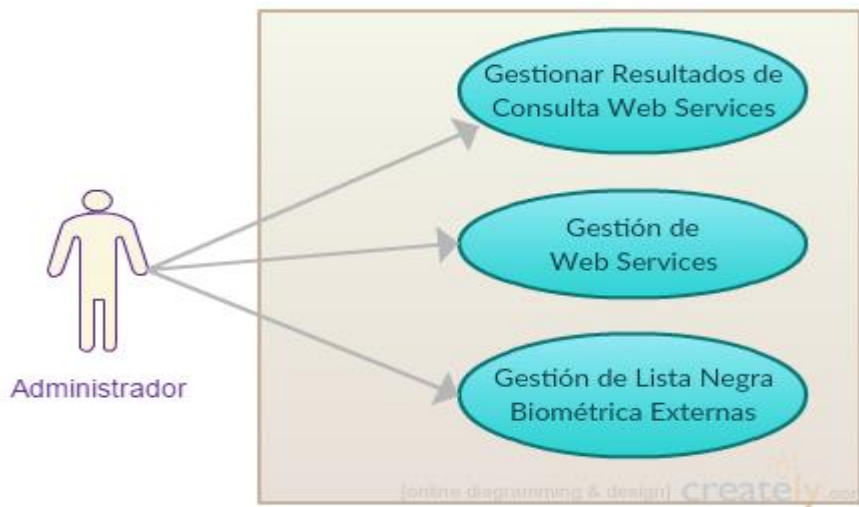
Los datos a ingresar son:

- Código (Numérico, 10) \*
- Descripción (Numérico, 100) \*

\* Todos los campos son obligatorios.



**CU: Gestión de Sistemas Externos**



**Gestionar Resultados de Consulta Web Services**

Que requieran derivación a Inspección Secundaria, el resultado será concatenado debajo del comentario agregado por el Inspector. Este resultado solo deberá ser visto en la pantalla de Inspección Secundaria cuando el Supervisor tome el caso.

Ejemplo:

En el campo 'Comentario' una vez que el Supervisor tome el caso para su evaluación deberá mostrarse:

"comentario de Inspector en Inspección Primaria..." + "WebServices Name" + "Resultado devuelto por el WebService"

**Gestión de Web Services**

En esta sección se podrán configurar los diferentes WebServices a los que el sistema se conectará para realizar las diferentes validaciones según correspondan.

Los datos a ingresar son:

- Código (Numérico, 10) \*
- Nombre (Alfanumérico, 100) \*
- Nombre a mostrar (Alfanumérico, 100) \*
- Cualquier otro dato necesario para la configuración de los WebService. \*
  - Ejemplo: IP y Puerto

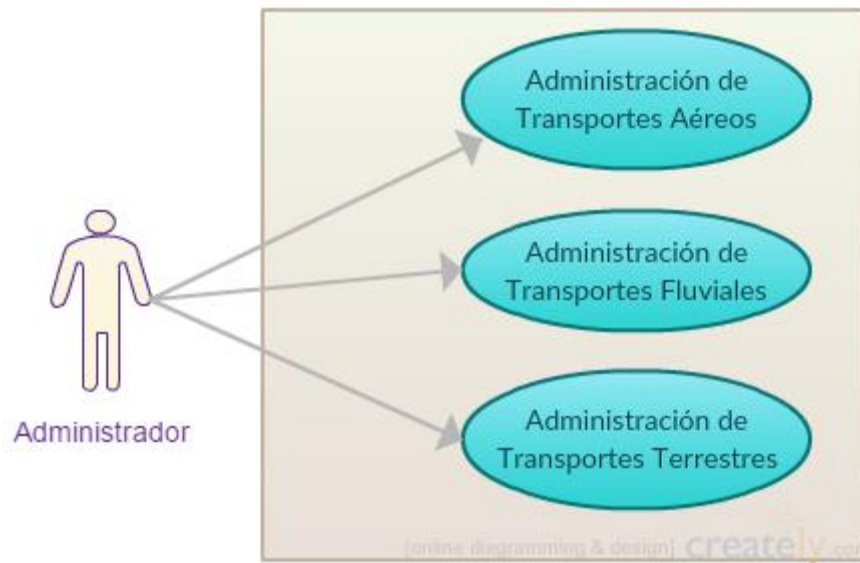
\* Todos los campos son de carácter obligatorio.

Las validaciones contra dichos Webservice serán realizados en la Inspección Primaria al momento de realizar el movimiento de Ingreso/Egreso del pasajero. Y los Webservice serán consultados por el Supervisor al momento de la Inspección Secundaria a través del botón "Validación contra Sistemas Externos" el que lo llevará a la pantalla correspondiente

### **Gestión de Lista Negra Biométrica Externas**

En caso de disponer de información para la Black List biométrica, se dispondrá de un AFIS en dónde estén registradas las huellas de las personas dentro de la Black List por lo tanto, cuando se registran las huellas de una persona, se realizará una búsqueda 1:N contra la Black List del AFIS.

### CU: Gestión de Transportes



#### Administración de Transportes Aéreos

Se darán de alta los códigos de vuelo que trabajan en el país y la dependencia, los cuales deberán ser denunciados por las empresas.

- Solo el usuario administrador puede cargar los códigos de vuelo de cualquier dependencia.
- Este requerimiento es un AMC y no requiere integración con otros sistemas.

Se debe ingresar:

- Compañía aérea (desplegable): proviene de Administración aéreas
- Arribo / Salida(desplegable) Se completara al momento de la Activación del transporte, según el movimiento
  - País Origen/Destino (Desplegable): Se completara al momento de la Activación del transporte.
  - Dependencia (desplegable): proviene de ABM dependencia
  - Numero de vuelo (alfanuméricos, 25)
  - Matricula de Vuelo (alfanumérico, 25) es un campo optativo, por default se mostrara #N/A

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá utilizar esta funcionalidad

Ejemplo

Para LAN: LP650... (Alfanuméricos)

### Administración de Transportes Fluviales

Se darán de alta las matrículas de los buques que trabajan en el país y la dependencia, los cuales deberán ser denunciados por las empresas.

- Solo el usuario administrador puede cargar las matrículas de los buques de cualquier dependencia.

- Este requerimiento es un AMC y no requiere integración con otros sistemas.

Se debe ingresar:

- Compañía fluvial(desplegable): proviene de Administración Fluviales
- Código OMI (alfanumérico, 50)\*: Será un desplegable y el sistema deberá permitir el ingreso si no existe el mismo.
- Arribo/Salida (desplegable) \* Se completara al momento de la Activación del transporte, dependiendo del movimiento.
- País Origen / Destino (desplegable)\* Se completara al momento de la Activación del transporte.
- Dependencia (desplegable)\*: proviene de ABM dependencia
- Matricula (alfanuméricos, 25)\*

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá utilizar esta funcionalidad

### Administración de Transportes Terrestres

- Solo el usuario administrador puede cargar esta información.
- Este requerimiento es un AMC y no requiere integración con otros sistemas.
- El Alta de los transportes terrestres particulares se realizará en la inspección primaria.

Se debe ingresar:

- Código Compañía Terrestre (desplegable): proviene de Administración Empresas Terrestres. (Para los casos particulares el código será PRV de Privado).
- Arribo / Salida (desplegable). Se completara al momento de la Activación dependiendo el movimiento.
- Patente (desplegable): Se completara al momento de la Activación del transporte.
- Marca: Se completara al momento de la Activación del transporte.
- Tipo de Vehículo: Se completara al momento de la Activación del transporte.

Controlar que solo exista una única patente por nacionalidad

Todos los campos son de carácter obligatorio al momento del ABM, y solo el usuario administrador podrá utilizar esta funcionalidad

## REQUERIMIENTO NO FUNCIONALES:



### CU: Performance

#### Tiempo de Respuesta

El trámite de registro de una persona en migraciones, entrante o saliente, no puede demorar más de 30 segundos para un flujo básico. Un flujo básico incluye lectura de pasaporte, captura 4-4-2 de huellas y venas, foto e iris.

La captura de documentación extra al documento de viaje, la recaptura de foto/iris, huellas y venas, la del documento de viaje y la recaptura de todos los datos cargados por el Supervisor quedan exceptuadas.

### CU: Usabilidad

#### Multibrowser

El sistema deberá ser "Multi-Browser", instalándose los drivers necesarios en cada puesto. Se utilizarán los browser: IE9 o superior y Chrome16 o superior.

### **Cambio de Campos por Medio de Teclas**

El sistema debe permitir que el usuario se mueva entre campos sin usar mouse, utilizando la tecla "tab".

Si la carga de los datos del pasajero se realizó en forma automática, es decir como resultado de la lectura del documento de viaje, el sistema deberá poner el cursor en el primer campo que es de captura manual.

Todas las pantallas posicionaran el cursor en el primer campo excepto que se especifique de otro modo como se realizó en Inspección primaria.

### **Refrescar Listado de Movimientos**

El sistema deberá realizar un refresco en la pantalla de inspección secundaria donde se listan los movimientos pendientes de una supervisión. De esta manera la información de los movimientos y sus estados se verán actualizados cada 30".

### **Sincronización de las Dependencias**

El Sistema de Control Migratorio deberá tener un mecanismo de sincronización para trabajar en un esquema en donde todas o algunas Delegaciones trabajen en forma local, sincronizando contra el Sistema Central.

- En el Sitio Central deberán de darse de alta todos los usuarios con sus roles y a qué dependencias pertenece. Sincronización desde el Sitio Central hacia las Dependencias

- Cada Dependencia administrará sus usuarios, por ejemplo cambio de puesto.

- El Sitio Central administrará los nomencladores, las Business Rules y la Black List (por Nro. Documento y Personas), Dependencias. Todo esto se sincroniza desde el sitio central hacia cada Dependencia (Nodo)

- Todo movimiento registrado en cada dependencia (Entrada/Salida) se sincronizará contra el Sitio Central.

- El sistema deberá operar de la misma forma, ya sea en una Delegación local, que en manera centralizada.

## CU: Seguridad

### **Impedimento para evitar puntos de control**

El sistema debe garantizar que un Inspector que esté realizando el registro de ingreso/egreso de persona, no pueda invalidar cualquier anomalía que haya detectado el sistema, y su única opción es enviar el pasaje a la supervisión de 2da línea.

Entiéndase como anomalía cualquier stop que el sistema genere a través de las validaciones que realiza en el documento de viaje, biometría o cualquier Business Rules que no cumpla el pasajero.

Es decir, si el sistema chequea que la persona está en Black List, el Inspector no podrá tomar otra opción en el sistema que no sea pasar a la persona a la supervisión de 2da línea, lo mismo si requiere Visa y no la tiene, u cualquier otro control del sistema. Es de carácter obligatorio el ingreso de un comentario del porque se está enviando a 2da línea, aparte de la causa.

El Inspector podrá enviar en cualquier momento del proceso de registro al pasajero a supervisión de 2da. Línea, donde tendrá que aparte de agregar un comentario seleccionar la causa del porque lo está enviando.

### **Unicidad de Roles**

Al momento de realizar el login al sistema, el mismo validara que el usuario posea solo UN rol, en caso contrario mostrará un mensaje indicando: "Inconveniente en Roles, comunicarse con el Administrador". Este mensaje será un Stop y no podrá ingresar el Sistema hasta la corrección de los Roles.

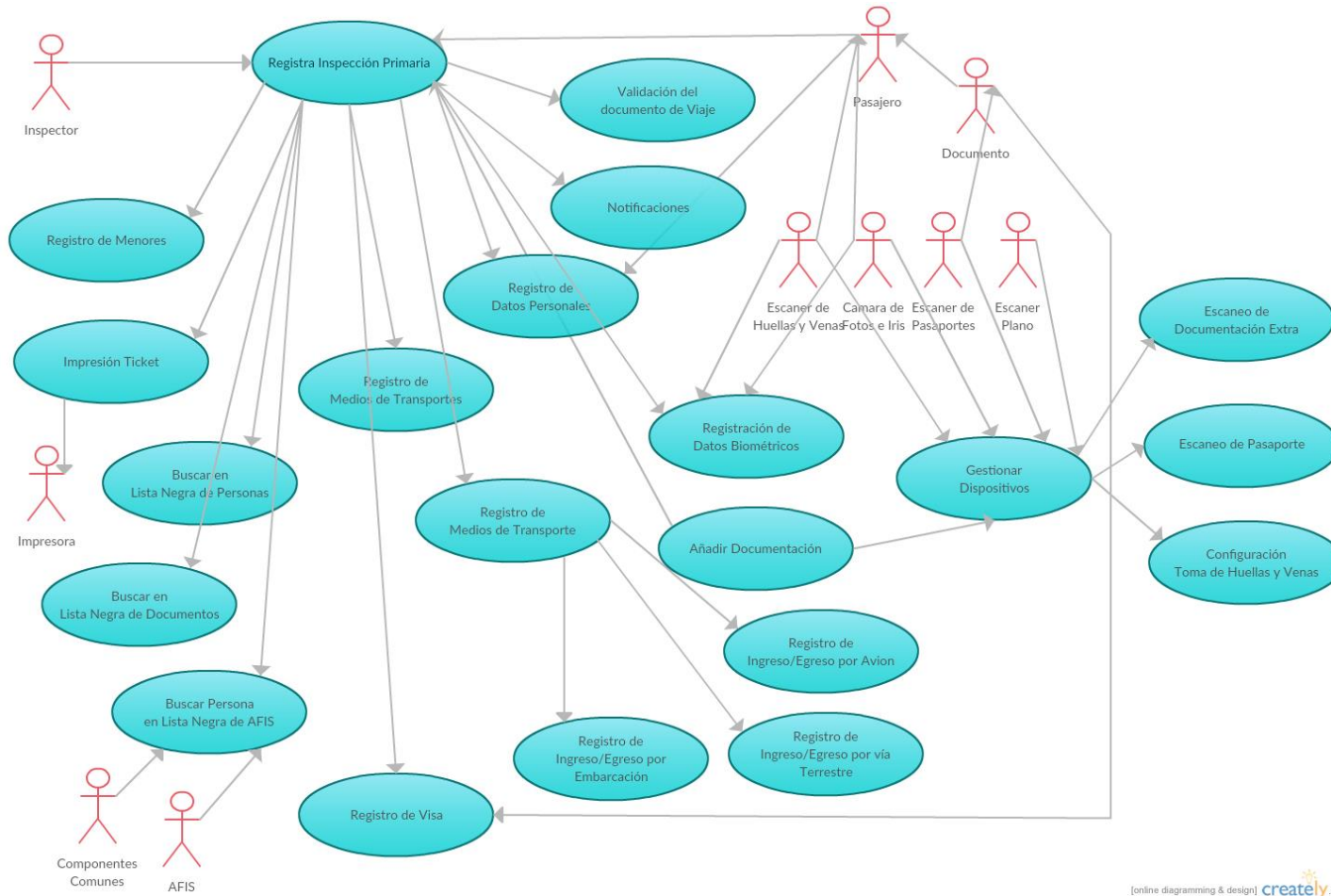
El sistema debe permitir configurar que esta validación sea realizada o no al momento del login.

### **Adaptación del Producto**

El producto deberá ser Internacionalizable. Idioma por default "Español".

## REQUERIMIENTOS FUNCIONALES

### CU: Inspección Primaria





## Inspección Primaria

Será el puesto donde el pasajero entregará el documento de viaje, y demás documentación necesaria para el ingreso/egreso del País. En caso de existir algún inconveniente se enviará a la Inspección Secundaria.

### Registro de Datos Personales

Se debe registrar de la persona:

- Apellido (texto) \*
- Otros Apellidos (texto)
- Nombre (texto) \*
- Otros nombres (texto)
- Tipo de documento (desplegable) \* Relacionado con el Nomenclador Tipo de Documentos.
- Número de documento (texto) \*
- Nacionalidad (desplegable) \*
- País emisor del documento (desplegable) \*
- Fecha de Nacimiento (fecha) \*
- Género (desplegable) \*

\* Son de carácter obligatorio.

\* Los países deben estar catalogados bajo el estándar ISO 3166-1 Alfa- 3.

\* CONTROL CONTRA SISTEMAS EXTERNOS

El sistema enviara a consultar los 'Arraigos', 'Antecedentes' y 'Ordenes de Captura' de la persona cuando el movimiento es de 'Egreso' y la misma es de la nacionalidad donde está el sistema implementado. La validación se enviara al momento de finalizar el ingreso de los datos personales de la persona, Nombre; Segundo Nombre; Apellido; Otros Apellidos, en

caso de haber coincidencia al momento de querer Finalizar el movimiento el sistema mostrara la pantalla "Derivar a Inspección Secundaria" con la causa 'Analizar Datos Personales'.

Todos los campos se completarán automáticamente cuando el Inspector realice el escaneo del documento de viaje. El sistema tendrá la opción para que el Inspector realice la carga de manera manual.

El Sistema deberá verificar cuando un apellido es compuesto o son dos apellidos, por ejemplo: "De la Fuente" deberá quedar en el campo "Apellido" y "Sánchez Rodríguez" deberá ser: Sánchez en Apellido y Rodríguez en Otro Apellidos

### **Registro del Medio de Transporte que Ingresa/Egresa**

De acuerdo al medio de transporte en que ingresó serán los datos a registrar.

El usuario se deberá loguear en el centro migratorio para el cual está habilitado, y ese centro migratorio deberá tener asociado el tipo de ingreso que recibe ("terrestre", "fluvial", "avión"), y de acuerdo a ese tipo sólo se le habilitará la opción de datos correspondiente al medio de transporte válido.

### **Registro de Ingreso/Egreso por Avión**

Si el medio de acceso es por avión, se deberá registrar la siguiente información:

- Aerolínea (desplegable): el usuario podrá seleccionarla del combo box o bien podrá ir ingresando carácter por carácter y el sistema ira mostrando por proximidad (autocompletar).
- Número de vuelo (desplegable / alfanumérico): si está cargado en el sistema el número de vuelo se selecciona, sino se permite su ingreso manual. El sistema dependiendo de la aerolínea hará un filtro por esta para mostrar los vuelos.
- Matrícula del Vuelo (alfanumérico).
- País de Origen/Destino (desplegable)

\* Todos los datos son de ingreso obligatorio.

### Registro de Ingreso/Egreso por Embarcación

En caso de ingreso/egreso por embarcación, se debe registrar la siguiente información:

- Empresa (Desplegable/alfanumérico): Si la empresa se encuentra cargada (y activa) el sistema mostrará la misma en el combo box para su selección.
- Identificación de embarcación (desplegable /alfanumérico): en caso de que la embarcación se encuentre registrada, el sistema la debe permitir seleccionar o bien podrá ir ingresando carácter por carácter y el sistema ira mostrando por proximidad (autocompletar).
- País de origen/destino (desplegable)

\* Todos los datos son de ingreso obligatorio.

### Registro de Ingreso/Egreso por vía Terrestre

En caso de ingreso/egreso por medio terrestre se debe registrar la siguiente información:

Pre selección:

- Empresa (Radio Button)
- Particular (Radio Button)
- A Pie (Radio Button)

Una vez que el Inspector seleccione el modo de ingreso terrestre el sistema habilitará los campos obligatorios a completar.

- Empresa (Desplegable)
- Placa (alfanumérico, 15).
- Marca (desplegable, 125) o bien podrá ir ingresando carácter por carácter y el sistema ira mostrando por proximidad.
- Tipo de Vehículo (desplegable).
- Nacionalidad

Todos los campos son de carácter obligatorio. Para Marca/Tipo de Vehículo se deberá cargar en un nomenclador (Administración Empresa Terrestre). El valor ingresado en "Placas" solo será de manera informativa y se guardara en el registro.

En la "pantalla de Ingreso Pasajero Terrestre" esta detallado para cada radio Button que valores deben ser obligatorios.

### Registro de Visa

El sistema utilizando la configuración, deberá determinar si la persona ingresante requiere Visa, a partir de su país de nacionalidad y tipo de documento. En caso de requerir Visa, se deben ingresar los siguientes datos:

- Número (alfanumérico, 256)\*
- Días permitidos de permanencia según Visa (alfanumérico).
- Consulado emisor (desplegable) (Proviene desde el Nomenclador de país): Que emitió la Visa (Se mostrará el listado de todos los países sin discriminar localidad, provincia, estado, etc.)
- Fecha de emisión (fecha)
- Fecha de vencimiento (fecha)

\* Todos los datos son de ingreso obligatorio.

### **CU: DERIVACION A INSPECCION SECUNDARIA**

En el contexto del proyecto, cuando el Inspector finalice el registro de inspección primaria y el movimiento requiera Visa (según la configuración, ej.: China - necesita Visa) y el sistema no tuviera conectividad contra el Webservice de VISAS, el sistema automáticamente mostrara la pantalla "Derivar a Inspección Secundaria" con la causa 'Validar Visa'.

Si el pasajero requiere Visa y no la tiene, no se puede continuar con el trámite de registro y se debe pasar al nivel de Supervisor de 2da línea.

## Registro de Menores

En el caso de menores residentes que salgan del país se deberá validar lo siguiente:

- Si el menor se encuentra acompañado por ambos padres, los mismos deben mostrar las partidas de nacimiento que validen su paternidad.
- Si el menor no es acompañado por sus padres, deben mostrar la solución judicial que autoriza el egreso del mismo del país.
- En caso de que el menor tenga una edad menor o igual a la configurada, se debe comprobar que vaya acompañado.
- En la pantalla 'Dirección General de Migraciones ~ Registro de Menores con acompañante' el Inspector deberá seleccionar uno de los dos radio Button que corresponden a la pregunta: "Acompañado por sus padres o mayor?"

En todos los casos, se debe indicar número de expediente u información comprobatoria de la validación en un campo de

Los posibles casos que pueden suceder en caso de salida de menores del país:

1. Padre acompaña y Madre acompaña (Deberá validarse que la solapa Madre y Padre posean personas seleccionadas)
2. Padre autoriza y Madre acompaña (Deberá validarse que la solapa Madre posea persona seleccionada y acta de autorización en solapa Padre)
3. Padre acompaña y Madre autoriza (Deberá validarse que la solapa Padre posea persona seleccionada y acta de autorización en solapa Madre)
4. Padre fallecido y Madre acompañante o autoriza (Deberá validarse que la solapa Madre posea persona seleccionada y acta en solapa Padre, en caso de que Madre autoriza deberá validarse Acta en solapa Madre y que solapa Tutor/Responsable posea persona seleccionada)
5. Madre fallecida y Padre acompañante o autoriza (Deberá validarse que la solapa Padre posea persona seleccionada y acta en solapa Madre, en caso de que Padre autoriza deberá validarse Acta en solapa Padre y que solapa Tutor/Responsable posea persona seleccionada)
6. Padre soltero y acta de nacimiento con hijo reconocido por el mismo en pestaña Madre (Validar que solapa Padre posea persona seleccionada y Acta ingresada en solapa Madre)

7. Madre soltero y acta de nacimiento con hijo reconocido por el mismo en pestaña Padre (Validar que solapa Madre posea persona seleccionada y Acta ingresada en solapa Padre)
8. Madre fallecida, padre fallecido y tutor acompaña (Deberá validarse que la solapa Padre y Madre posean Acta ingresada, y que la solapa Tutor/Responsable posea persona seleccionada y tipo de presencia acompaña)  
NOTA: el proyecto no debe permitir confirmar un registro de menor con:
9. Madre fallecida, padre fallecido y tutor autoriza (un menor siempre debe salir acompañado)

### **Registración de Datos Biométricos**

En el momento de la registración de la persona se deberá registrar:

- Huellas (4-4-2): para los casos en que la persona no estuviera registrada en el sistema, se capturan todas las huellas que tenga la persona.
- Huellas (4): en caso que la persona está registrada y el sistema estuviera configurado para validar con 4 dedos.
- Huellas (2): en caso que la persona está registrada y el sistema estuviera configurado para validar con 4 dedos.

Calidad de huellas

- En caso de que una huella no cumpla con el mínimo de calidad, se mostrará la huella con un recuadro en colorado y se realizará una recaptura.
- La calidad mínima de captura de huella deberá estar basada en dos estándares:
  1. NFIQ (NIST Estándar NISTIR 7151)
  2. IQL (Nec Estándar)

NFIQ tiene valores de 1 a 5 y el IQL valores de 0 a 100, ambos configurables para cada dedo. Entonces, debería considerar:

- Si NFIQ fuera de Valores permitidos entonces “Calidad Mala”
- Si NFIQ dentro de Valores permitidos y si no tiene IQL configurado entonces “Calidad OK”

- Si NFIQ dentro de Valores permitidos, si tiene IQL configurado y dentro de Valores permitidos entonces “Calidad OK”
- Si NFIQ dentro de Valores permitidos, si tiene IQL configurado y fuera de Valores permitidos entonces “Calidad Mala”
- La cantidad de reintentos para realizar una captura de huellas, deberá ser configurable. La configuración es de reintentos por huella.
- En caso de que el pasajero no posea ninguna de las 2 manos o los 10 dedos faltantes (amputado), se deberán destildar todos los Check correspondientes a los dedos.
- En caso de que sea imposible la captura de alguno de los dedos, sea esto por estar vendado, lastimado se tratará como ausente seleccionando en la pantalla el Check correspondiente.

Al momento de crear la persona en BU se comprobarán los siguientes escenarios:

- 1) En caso de no existir la persona en Base Única se dará de alta con sus datos demográficos y biométricos.
- 2) En caso de existir la persona y haber "clones" se derivará a Inspección Secundaria al finalizar el registro de la Inspección Primaria con el motivo "Posibles Clones". Donde el Supervisor al dar click sobre el botón "Biometría Cruzada" se le presentará la pantalla desde Componentes Comunes con los posibles candidatos que ya existen en BU.

Los controles ICAO deberán ser configurables.

- El formato de la captura de iris, es el definido por biometría en Componentes Comunes.
- Para el caso de niños, bebés o personas que no puedan fijar la vista serán enviados al Supervisor. En caso de personas que no posean ninguno de los dos ojos, deberá el Inspector tildar los dos Check correspondiente cada uno a cada ojo.

### Configuración Toma de Huellas y Venas

Se deberá poder configurar la toma de huellas dactilares y venas. Esto refiere a que si el pasajero ya posee movimientos migratorios se deberá poder configurar (dependiendo cada país) la toma de las huellas. Siendo 4-4-2 la primera vez y luego solamente 4 o 2. Y para las huellas de las venas La primera vez se tomarán de ambas manos, y luego solo se contemplará la configurada

- En caso de configurar 2, serán los pulgares y las venas de las manos derecha
- En caso de configurar 4, será el meñique, anular, medio e índice de la mano derecha y las venas de las manos derecha.

### Escaneo de Pasaporte

A través del escáner de pasaporte se deberá permitir escanear la imagen del pasaporte y guardar adjunta al registro de ingreso/egreso.

### Validación del documento de Viaje

En caso de ser Automático, a partir de las librerías aportadas por el escáner de pasaporte, se deberá verificar la validez del documento de viaje:

- Se debe hacer verificaciones cruzadas de los datos en el Smart chips contra el documento (MRZ vs Smart chip, se deberán controlar todos los datos), y prueba de información para consistencia de formato a modo de confirmar la autenticidad del mismo.
- Verificar los datos del Smart chip de los e-Passport y de la MRZ (zona de lectura mecánica) la suma de control, controlar la fecha de vencimiento, y confirmar la presencia de tinta.
- Capturar una gama completa de imágenes en color del documento usando fuentes de luz visible, infrarroja y ultravioleta, proporcionando un registro visual tanto de la información visible como de la leída mecánicamente.
- En caso de que alguna de las validaciones fallara se enviará a inspección secundaria.



- Se realiza cruce contra Black List, y en caso de dar positivo se enviará a inspección secundaria.
- La Fecha de Vencimiento deberá ser editable aunque el ingreso/egreso del movimiento haya sido realizado por Scanner.

En caso de que el ingreso sea manual, solo se validará

- La fecha de vencimiento del pasaporte. (GG- En caso de ser manual, se validara visualmente la Fecha de Vto.)

### **CU: VALIDACIONES CONTRA SISTEMAS EXTERNOS**

Si el ingreso del documento de viaje es manual o por medio del lector de pasaporte se deberá realizar la verificación contra el Registro Nacional.

#### **En caso de no haber conectividad contra los Webservice**

Cuando el Inspector Finalice el registro de inspección primaria:

Validación de documento nacional:

- si el tipo de documento de la persona es DNI Propio de la Nación Involucrada, consultar Webservice y comparar datos demográficos obtenidos contra los ingresados en pantalla y en caso de no coincidencia de algún campo, mostrar la pantalla para derivar a inspección secundaria con la causa de derivación "Diferencia de información demográfica".

Validación de pasaporte nacional:

- si el tipo de documento de la persona es Pasaporte y el país emisor, consultar Webservice Pasaporte nacional y comparar datos demográficos obtenidos contra los ingresados en Interfaz y en caso de no coincidencia de algún campo, mostrar la interfaz para derivar a inspección secundaria con la causa de derivación "Diferencia de información demográfica".

## WebService Pasaporte extranjero

### Validación residencia

- Si la categoría migratoria seleccionada es Residente en una inspección primaria de ingreso, consultar Webservice Pasaporte extranjero para verificar si la persona tiene residencia emitida.
- En caso de que la respuesta sea que tiene residencia, el sistema mostrarán los datos obtenidos en pantalla.
- En caso de que la respuesta sea que no tiene residencia, el sistema mostrará una advertencia en pantalla para enviar a Supervisor. Mostrar la interfaz para derivar a inspección secundaria con la causa de derivación "No tiene residencia".

<b>Impresión Ticket</b>
-------------------------

En caso que el pasajero no posea un documento de viaje donde poder sellar el ingreso al país, el Inspector podrá imprimir un ticket que el mismo deberá ser entregado al momento de salir del país.

Los campos que deben estar en el tiquete son:

- Apellido y Nombre
- Nro. Documento de viaje
- Nacionalidad
- Dependencia
- Fecha Ingreso (sysdate)
- Fecha Egreso (Esta deberá ser según la categoría de ingreso, el sistema deberá calcular según el valor que el Inspector ingrese, sysdate + cantidad de día.)

Todos los campos son los ingresados en la pantalla de ingreso. Se maneja un formato XML para la impresión del tiquete.

### Notificaciones

El sistema deberá ir mostrando las notificaciones/alertas para el movimiento que se está realizando. El Inspector deberá ir tildando las mismas para que el sistema le permita "Finalizar el Registro". El sistema debe registrar las notificaciones.

Según el alerta/notificación que haya en la lista, al presionar "Finalizar Registro" el movimiento pasa o se envía a segundo nivel (Supervisor).

Por Ejemplo:

Si una alerta muestra que huellas, rostro y/o iris dio hit contra Black List biométrica y el Inspector tilda como vista la misma y da Finalizar Registro, el sistema automáticamente enviara el caso al Supervisor. (A modo de ejemplo esto)

### Escaneo de Documentación Extra

Para el caso de los menores residentes que deseen salir del país, el Inspector deberá escanear los documentos.

En caso de que alguno de estos documentos no se presenten, se enviará a inspección secundaria.

También podrá escanearse y guardarse cualquier tipo de documentación que el Inspector crea necesaria

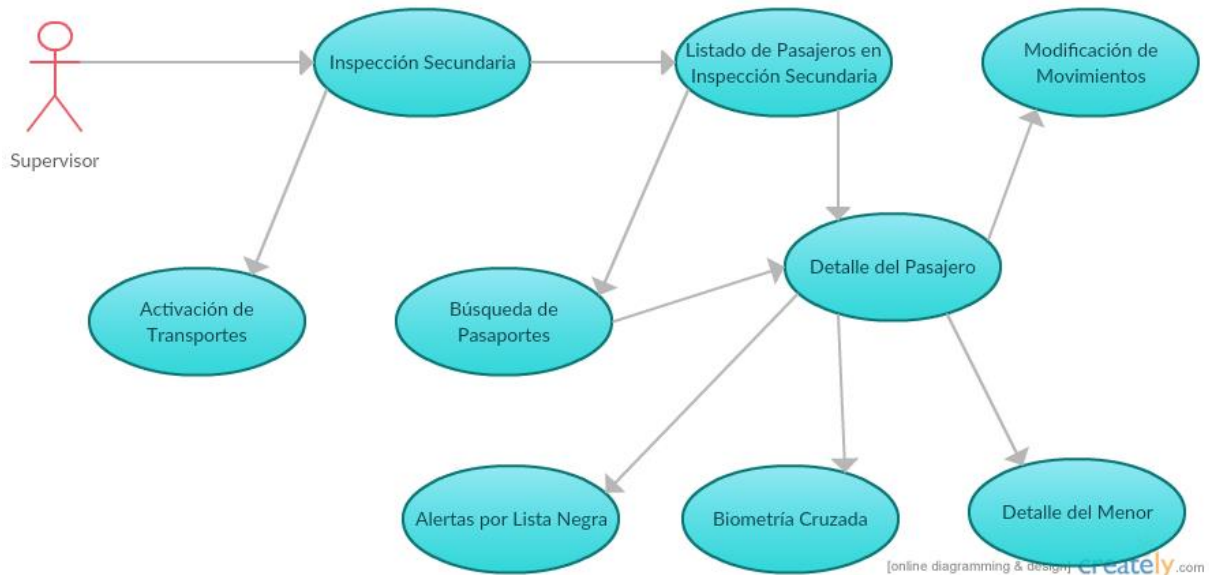
### INPUT/OUTPUT

Dispositivo:

- Escáner de Pasaportes:
  - Input será el escaneo del pasaporte una vez insertado para su lectura y análisis.
  - Output: Se espera que el escáner devuelva hacia la página los siguientes valores:

- Verificaciones cruzadas de los datos en el Smart chips contra el documento, y prueba de información para consistencia de formato a modo de confirmar la autenticidad del mismo.
- Verificar en forma cruzada la información entre la MRZ y los datos del Smart chip, y a través de múltiples documentos en un conjunto.
- Verificar los datos del Smart chip de los e-Passport y de la MRZ (zona de lectura mecánica) la suma de control, controlar la fecha de vencimiento, y confirmar la presencia de tinta.
- Capturar una gama completa de imágenes en color del documento usando fuentes de luz visible, infrarroja y ultravioleta, proporcionando un registro visual tanto de la información visible como de la leída mecánicamente.
- A parte de los datos de la persona, Apellido, Otros Apellidos, Nombre, Otros Nombres, Fecha de Nacimiento, Nacionalidad, Tipo y Numero de documento, Fecha de Vencimiento del documento, sexo

### CU: Inspección Secundaria



#### **Inspección Secundaria**

El Supervisor atenderá todos los pasajeros que no pasaron por la inspección primaria.

#### **Listado de Pasajeros en Inspección Secundaria**

El Supervisor verá un listado con todos los pasajeros que fueron enviados a Inspección Secundaria que aún no fueron inspeccionados. El Supervisor podrá seleccionar un pasajero del listado para realizar la supervisión. Los casos pasados a Inspección Secundaria solo podrán ser resueltos y vistos por los supervisores logueados en la misma dependencia del caso.

El listado mostrará por cada pasajero:

- Tipo y numero de documento
- Nacionalidad
- Movimiento: (ingreso o egreso)
- Motivo de inspección

Posible escenarios para el caso de que un movimiento este asignado a un Supervisor y el browser se cerrase, solo el mismo Supervisor podrá continuar con la resolución del caso, si otro Supervisor quisiese tomarlo el Sistema mostrar un warning indicando que el caso está siendo resuelto por el Supervisor

### Detalle del Pasajero

El Supervisor al seleccionar un pasajero del listado, el sistema mostrará el detalle del mismo junto a la causa y al comentario del Inspector del por qué es necesario Inspección Secundaria, donde el Supervisor podrá Autorizar o no el ingreso/egreso del Pasajero.

### Biometría Cruzada

La funcionalidad en cuestión será utilizada en Inspección Secundaria por haber dado Alerta en alguna de las comparaciones de los clones encontrados por Componentes Comunes al intentar crear/comparar una persona. El proyecto deberá mostrar un listado de los posibles 'clones' con los siguientes datos:

- Nro. Documento
- Apellido/s
- Nombre/s
- Sexo
- Fecha de Nacimiento
- Foto (en caso de poseerla en Componentes Comunes)
- Resultado de comparación de huellas

El Supervisor al momento de seleccionar uno de los clones tendrá la posibilidad de:

- 1) Actualizar el registro en Componentes Comunes de la persona.
- 2) Forzar la creación de una nueva persona en Componentes Comunes.
- 3) En caso de 'Fraude' no se creara la persona en Componentes Comunes.

### Alertas por Lista Negra

En caso de haber pasado a supervisión por haber dado hit contra Black List (Persona, documento, y biométrica) este botón se habilitara para que el Supervisor pueda ver en forma de grilla (mostrada en un pop up) los posibles match que dio en la inspección.

## Activación de Transportes

En la pantalla general de 2do nivel se mostrara la opción para la activación/desactivación de transportes. El sistema según la dependencia deberá mostrar la activación de transporte correspondiente: Aéreo, fluvial o Terrestre.

El caso de Aéreos y Fluviales se podrá realizar activaciones programadas a futuro.

Cuando se trate de una Activación de un transporte Aéreo, el Supervisor deberá seleccionar:

- Aerolínea
- Nro. de Vuelo

Y deberá ingresar los siguientes valores:

- Matricula de Vuelo (en caso de que se conozca sino dejara el valor #N/A por defecto)
- País Origen / Destino (según sea el movimiento)

Para el caso de Transporte Fluvial, el Supervisor deberá seleccionar:

- Empresa
- ID Embarcación (será la matrícula de la embarcación)

Y deberá ingresar el siguiente valor:

- País Origen/Destino (según sea el movimiento)

Para el caso de transportes terrestres existen 2 tipos de tratamientos:

- Empresas y Particulares.

Las Empresas estarán previamente cargadas y el Supervisor deberá seleccionar:

- Empresa

Y deberá ingresar los siguientes datos:

- Marca
- Matrícula del vehículo
- Nacionalidad del Vehículo
- Tipo de vehículo.

Cuando el transporte terrestre sea particular el Supervisor deberá seleccionar la empresa "PRV" del combo 'Empresa', los datos a ingresar serán el mismo que en el caso anterior, pero la nacionalidad que se guardara en la base de datos será la misma para Nacionalidad Empresa y Nacionalidad Vehículo.

## Búsqueda de Pasaportes

Se ingresa el documento de viaje o parte del mismo y se presiona "Buscar", el sistema mostrara un pop con los posibles candidatos. El Supervisor seleccionara de ese pop up el movimiento que desea modificar y a continuación presiona el botón "Modificar Movimiento". El sistema luego de que el Supervisor acepta la modificación del movimiento lo lleva a la pantalla

Los filtros para buscar personas será:

- Tipo de Documento
- Nro. de documento de viaje (parte o completo)

No es obligatorio el ingreso de los 2 campos, con uno de ellos es suficiente para enviar la búsqueda.

Puede ser un movimiento de ingreso o egreso del mismo día o de días, meses o años anteriores. Realizando la búsqueda por el nro. De documento de viaje (completo o parte del mismo), Nombre y Apellido, Rango de Fechas, y presionando "Buscar". Si el Supervisor ingreso el Documento de viaje completo el sistema mostrará el listado de los movimientos del pasajero para que seleccione el que quiere modificar, si el Supervisor ingreso solo parte del documento el sistema mostrara un listado con los posibles candidatos, al seleccionar el que corresponda mostrara el listado de los movimientos. En ambos casos si el pasajero no posee un histórico de movimientos el sistema directamente pondrá en contexto el único movimiento de dicho pasajero,

## Modificación de Movimientos

Este requerimiento es utilizado por el Supervisor en caso de que algún movimiento ya registrado y procesado necesite algún cambio. Puede ser un movimiento de ingreso o egreso del mismo día o de días, meses o años anteriores. Realizando la búsqueda por tipo y el nro. De documento de viaje (completo o parte del mismo) y presionando "Buscar". Si el Supervisor ingreso el Documento de viaje completo el sistema mostrará el listado de los movimientos del pasajero para que seleccione el que quiere modificar, si el Supervisor ingreso solo parte del documento el sistema mostrara un listado con los posibles candidatos, al seleccionar el que corresponda mostrara el listado de los movimientos. En ambos casos si el



pasajero no posee un histórico de movimientos el sistema directamente pondrá en contexto el único movimiento de dicho pasajero.

Los datos que se podrán modificar del pasajero serán sus datos demográficos, datos del medio de transporte, no se podrá modificar el tipo de transporte; nro. De documento de viaje, Categoría Migratoria, Días de permanencia, como también los datos de la Visa en caso de haberse ingresado (Nro. Visa, fecha de Nacimiento, País Emisor, tipo de Visa). Los datos biométricos no podrán modificarse.

Al presionar el botón "Log de Estados" el sistema devolverá todos los movimientos del pasajero y sus estados, los datos serán mostrados en una grilla de la siguiente manera:

Fecha y hora	Nro. Documento	Apellido y Nombre del pasajero	Nacionalidad	Nombre Completo Inspector	Estado del movimiento	Dependencia/Puesto	Motivo de la modificación
--------------	----------------	--------------------------------	--------------	---------------------------	-----------------------	--------------------	---------------------------

"esquema de trazabilidad donde damos de baja de forma lógica el registro original, lo vínculo con el nuevo registro (el modificado) y le sumo datos de auditoría como ser IP+Operador+Fecha+Hora. De esta forma mantenemos el origen y trazamos la relación con sucesivas modificaciones. Este esquema no pierde el movimiento original y permite rearmar la historia ante cualquier necesidad operativa. Además lleva un control de los responsables de dichos cambios, los movimientos modificados quedaran en la base con el estado "Modificado" y linkeados al nuevo movimiento"

#### **Detalle del Menor**

Si el registro que se está visualizando pertenece a un menor, cualquiera sea el rango, el botón se habilitará y el Supervisor podrá ver los datos registrados para el menor, sean estos actas, padre y madre linkeados. Si el menor se encuentra en el rango de 0-6 mostrara de forma solo lectura.

## DISCUSIÓN

Es requerido que el análisis acompañe el desarrollo durante toda la vida del proyecto ya que los dispositivos biométricos son utilizados regularmente pero ellos contemplan un avance tecnológicos y por lo tanto cambios en los procedimientos actuales utilizados por los controles migratorios, por lo cual pueden contemplar muchas funcionalidades no contempladas originalmente, y por lo tanto muchos desvíos no previstos, las buenas prácticas no recomiendan ser estrictos en las definiciones dado que muchas veces se puede incurrir en desarrollar lo originalmente detectado pero que no conforme al cliente, por tal motivo con este diseño se intenta complementar dichas posibles deficiencias desarrollándose en conjunto con los analistas, las definiciones de los Onwer Product y Key Users de las áreas involucradas y los Gerentes Sponsor que tomaron la decisión de llevar adelante la inversión en el desarrollo, sin olvidar hacer foco en un buen equipo de QA (Quality Assurance) que garantice la calidad del desarrollo.

También es requerido el desarrollo sea contemplado en la realidad actual de cada país, dado que no se debe exceder en el control pero tampoco deberá ser insuficiente para detectar inequívocamente una persona, porque así como se corre el riesgo de dejar pasar un potencial peligro para cualquier Nación, también se corre el riesgo de acusar sin justificativos y falsamente, e incurrir así en injurias.

El movimiento migratorio en cualquier país es un tema sensible y posibles conflictos entre las naciones soberanas, por ello un buen control como el planteado en este desarrollo es fundamental para evitar los malos entendidos y no es muy invasivo sobre los evaluados para no generar susceptibilidades innecesarias.

## Capítulo 5

### PLAN DEL PROYECTO

La presente planificación tiene como objetivo establecer los fundamentos que regirán la ejecución del Proyecto Control Migratorio, como ser la organización del proyecto (Equipo de proyecto, roles, etc.), alcance, cronograma, entregables, la estrategia de ejecución, control del avance, control de cambios, etc.

Esta es un documento vivo por lo tanto evolucionará durante el ciclo de vida del proyecto como así también la documentación asociada a este plan.

Este proyecto se encuentra enmarcado en la contratación de Consultoras Profesionales para la ejecución de un proyecto de desarrollo de software para gestionar el control migratorio. El proyecto tiene una duración de 9 meses de desarrollo, 3 meses de implementación, capacitación y prueba piloto en un aeropuerto significativo, y conjuntamente con el feedback correspondiente entonces la adecuación y la implementación en el resto de los puestos fronterizos a lo largo de 2 años más.

El proyecto tiene como objetivo el desarrollo e implementación de una solución de software para llevar a cabo el control migratorio, en todos sus puestos fronterizos.

El proyecto principal será gestionado el gobierno que contrató en una consultora externa los siguientes servicios.

El proyecto incluye:

- ✓ Consultoría Inicial de Procesos
- ✓ Provisión de Licencias de Software y AFIS
- ✓ Servicios de Desarrollo del Producto (análisis, diseño, programación, etc.)
- ✓ Puesta en Marcha
- ✓ Capacitación en el uso a usuarios finales y administradores.
- ✓ Servicios de Soporte Técnico de 3er nivel durante el lapso de 6 años a partir de la Aceptación del Producto.
- ✓ Provisión de Documentación Técnica, Manuales, etc.

## **DESCRIPCIÓN DE LOS PRODUCTOS Y SERVICIOS**

A continuación se describen los productos y servicios a proveer en el marco del proyecto.

### **Software:**

Se proveerá la herramienta de control migratorio, constará de los siguientes módulos, cada uno de ellos con las funcionalidades que se detallan a continuación:

- Registro de pasajeros: permitirá registrar los datos de los todos los pasajeros que arriben por cualquier medio.
- Validación de Documento de Viaje: se registra la imagen escaneada de los pasaportes y la validez del mismo. Para ello se utiliza el lector de pasaportes RealPass.
- Registro de datos de Visa: en caso que sea requerida para el ingreso, se registrará la imagen escaneada y datos de la Visa del pasajero.
- Registro de datos biométricos del pasajero:
  - Huella dactilar y venas: se registrarán los 10 dedos de los pasajeros y las venas de la palma de la mano a elección (según parámetros).
  - Rostro e iris: se registrará la imagen del rostro del pasajero y los datos biométricos del iris de dicho pasajero mediante una cámara especial (iCAM TD100)
- Administración de Black List: es una lista de personas buscadas que es provista por entes externos. Durante el proceso de registración, se verifica si la persona está incluida en dicha lista y se avisa al operador para que actúe de acuerdo a los procedimientos definidos para estos casos.
- Administración del sistema: permitirá la Gestión de Usuarios y permisos de acceso, copias de seguridad, actualizaciones de Black List, etc.

- Módulo de Consultas e Informes
- Módulo de Informes Estadísticos
- Integración con sistemas externos: serán implementados a través de Web Services.

### Capacitación:

Con el objetivo de garantizar el entrenamiento en el uso de la herramienta se brindará capacitación a los diferentes usuarios de la misma.

Dicha capacitación se realizará en el sitio que el gobierno disponga. Los destinatarios de la misma serán definidos por el mismo gobierno. En principio se capacitará a usuarios administradores y formadores de usuarios finales.

### Supuestos

- El gobierno proveerá las instalaciones donde llevar a cabo la capacitación en tiempo y forma.
- El Plan de Capacitación se adecuará en cuanto a fechas definitivas y audiencia, a medida se aproxime la fecha fijada en el cronograma, en acuerdo con el gobierno.

### **DESPLIEGUE Y PUESTA EN MARCHA**

Las actividades de puesta en marcha comprenden:

- Despliegue de la Solución en Data Center: se realizará en dos etapas. En la primera se instalarán los módulos de administración y registro de pasajeros. En la segunda etapa, se desplegarán los módulos de Black List, consultas y estadísticas.
- Puesta en marcha: contempla la implementación de más de 100 puestos de control. En la primera etapa se implementarán los correspondientes al Aeropuerto Principal del Territorio Nacional. En una segunda etapa, todos los restantes.
- Durante la puesta en marcha, se brindará soporte en sitio, acompañamiento operacional hasta lograr la estabilización de la operación del sistema y de los procedimientos de control y registro.

#### **Soporte:**

Se provee el Servicios de Soporte Técnico de 3er nivel durante el lapso de seis años, partir de la aceptación y puesta en marcha del primer sitio. Dicho servicio de soporte será brindado dentro del horario de oficina, considerándose el mismo, de Lunes a Viernes de 9 a 18 hs Fuera de éste horario, se prevé la modalidad de "guardias pasivas", dedicando líneas móviles para acceder al personal de Asistencia Técnica.

#### **Documentación**

Se proveerá la siguiente documentación al inicio del proyecto

- ✓ Especificación General de Requerimientos Funcionales
- ✓ Especificación de Requisitos para Configuración de Data Center

Se proveerá la siguiente documentación al final de cada etapa:

- ✓ Manual de Instalación
- ✓ Manual del Usuario
- ✓ Plan de Aceptación

## **METODOLOGÍA DE IMPLEMENTACIÓN**

Se ha dividido el proyecto en tres fases, más una etapa de iniciación que a continuación se describen:

- **Fase 1 (duración nueve meses)**
  - ✓ Consultoría de Procesos
  - ✓ Definición del alcance definitivo etapa 1
  - ✓ Desarrollo de la Solución (Etapa 1)
  - ✓ Despliegue de la Solución
  - ✓ Capacitación
  - ✓ Puesta en Marcha en Aeropuerto “A Designar”
  
- **Fase 2 (duración tres meses)**
  - ✓ Definición del alcance definitivo Etapa 2
  - ✓ Desarrollo de la Solución (Etapa 2)
  - ✓ Despliegue de la Solución
  - ✓ Capacitación
  
- **Fase 3 (duración dos años)**
  - ✓ Puesta en Marcha en los sitios restantes
  
- **SopORTE (duración seis años)**

## **ENTREGABLES DEL PROYECTO**

A continuación se resumen los entregables del proyecto.

### **Software**

- ✓ Informes de Consultoría de Procesos
- ✓ Sistema de Control Migratorio

### **Servicios:**

- ✓ Capacitación de Administradores del Sistema
- ✓ Capacitación de Usuario y/o Formadores

### **Documentación:**

#### **Inicio**

- Plan de Proyecto
- Requerimientos Funcionales
- Especificación de Configuración de Data Center

#### **En cada Liberación**

- Manual de Instalación
- Manual del Usuario
- Plan de Pruebas de Aceptación

#### **Cierre**

- Informe de Cierre

### **Garantía y Mantenimiento correctivo**

- Soporte por 6 años



## **CONTROL DE CAMBIOS**

El objetivo del procedimiento de Control de Cambios es el de establecer un mecanismo formal de identificación, propuesta, evaluación, discusión y aprobación o rechazo de cualquier al proyecto que afecte a los costos, tiempo o alcance.

Se entiende por cambio a todo aquello que produzca una variación en los productos, en los servicios, en la modalidad, en el plan de proyecto, en las obligaciones mutuas, es decir, en todo aquello que difiera de lo previsto contractualmente.

El presente procedimiento define claramente los pasos necesarios para manejar una Solicitud de Cambio, como así también define las personas u organizaciones involucradas en el mismo con sus respectivas responsabilidades.

La meta principal del procedimiento es permitir el desarrollo ordenado de las actividades e interacciones entre el Proyecto y la Consultora que desarrollará el software, a través de:

- ✓ La implementación única de los cambios aprobados,
- ✓ El conocimiento del impacto de cada cambio en el proyecto,
- ✓ El seguimiento de los cambios identificados,
- ✓ El registro histórico de los cambios en el proyecto.

El apego estricto a lo normado por este procedimiento redundará en los siguientes beneficios para el proyecto:

- ✓ Administrar y formalizar todos los cambios a especificaciones del Proyecto y nuevos requerimientos.
- ✓ Realizar el adecuado seguimiento de cada una de las solicitudes.
- ✓ Evaluar oportunamente el impacto técnico, los riesgos de la implantación, el costo e impacto financiero de un cambio o nuevo requerimiento, y tomar las decisiones adecuadas.
- ✓ Precisar el alcance funcional de cada versión y su fecha de entrega.
- ✓ Obtener oportunamente el apoyo técnico para la implantación efectiva del cambio.

- ✓ Permitir la verificación del cumplimiento de los entregables con los requerimientos acordados.
- ✓ Mejorar la planeación y el control del Proyecto.
- ✓ Mantener en forma clara, objetiva y sin ambigüedades los cambios al Cronograma y al Proyecto en general.

### **PLAN DE CAPACITACIÓN**

La capacitación está destinada al personal de la Dirección de Migraciones del país que desarrollará el control, considerando el rol que cumplen en la misma. Por ello, se dictarán tres tipos de cursos, según estén dirigidos a Inspectores, Supervisores y Administradores.

La capacitación estará divididas en dos etapas: una antes de la puesta en marcha y otra cuando se incorporen las funcionalidades que no están presentes en la primera versión del producto.

Así mismo, en una primera fase, sólo se capacitará al personal del Aeropuerto Principal. Luego, cada etapa de la capacitación, se efectuará con el resto del personal (puestos terrestres y fronterizos).

#### **Supuestos y Requisitos**

Es presenta plan está desarrollado considerando las siguientes suposiciones:

- Se deberá contar con una sala al menos 5 puestos de trabajo (con todos sus dispositivos conectados)
- Acceso al Producto desde la sala de capacitación.
- Un puesto de trabajo extra para el Capacitador, que además posea un Proyector.
- Se consideran 2 asistentes por puesto de trabajo.

### **Capacitación a Administradores**

**Duración:** 20 horas

**Cantidad de Cursos:** 1

**Máximo número de asistentes:** 5

#### **Objetivo**

Formar al personal de la Dirección General de Migración que da soporte de primer nivel, configuración y administración, mantenimiento preventivo y correctivo de la solución Propuesta.

El personal técnico será entrenado para mantener la solución operativa. Incluye "prácticas profesionales", tareas durante la primera puesta en marcha del sistema y los siguientes elementos:

- Instalación Solución Propuesta.
- Configuración Solución Propuesta.
- Administración de Listas Negras o impedimentos.
- Configuración de parametrización de la solución.

### **Capacitación a Supervisores**

**Duración:** 20 horas.

**Cantidad de Cursos:** 3

**Máximo número de asistentes:** 10 (*considerando que para las delegaciones del interior se organizaran eventos en la ciudad principal de la Nación que implementará el proyecto*).

#### **Objetivo:**

Preparar al personal de la DGM que deberá utilizar la solución del proyecto en las siguientes funcionalidades:

- Procedimiento de Inspección Primaria en controles Aéreos, Marítimos y Terrestres
- Procedimiento de Inspección Secundaria.
- Utilización de los diferentes dispositivos requeridos para las inspecciones.

### **Capacitación a Inspectores**

**Duración:** 16 horas.

**Cantidad de Cursos:** 12

**Máximo número de asistentes:** 10 (*considerando que para las delegaciones del interior se organizaran eventos en la principal ciudad de la Nación*).

**Objetivo:**

Preparar al personal de la DGM que deberá utilizar la solución en las siguientes funcionalidades:

- Procedimiento de Inspección Primaria en controles Aéreos, Marítimos y Terrestres
- Utilización de los diferentes dispositivos requeridos para las inspecciones.

### **Material**

**Destinatarios:**

**ADMINISTRADORES**

- Manual de Instalación y Configuración.
- Manual del usuario del Producto.
- Presentación de Administración.
- Documento de Ejercicios.

**SUPERVISORES**

- Manual del usuario del Producto.
- Presentación de Procedimientos de Inspección Primaria y Secundaria.
- Documento de Ejercicios de Inspección Primaria y Secundaria.

**INSPECTORES**

- Manual del usuario del Producto.
- Presentación de Procedimientos de Inspección Primaria.
- Documento de Ejercicios de Inspección Primaria.

## **COMUNICACIONES DEL PROYECTO**

### **Informe de Avance del Proyecto:**

Con el fin de mantener informado al Cliente del estado de avance del proyecto se enviará un informe semanal con el estado de avance. Este informe será confeccionado por el Gerente de Proyecto.

El contenido estándar de los temas a incluir en el informe son:

- Avance de las actividades.
- Compromisos pendientes.
- Cambios al proyecto.

### **Informe de Avance del Proyecto Interno**

Con el fin de mantener informado al equipo de proyecto del estado de avance del mismo, se generará un informe semanal con el estado de avance. Este informe será confeccionado por el Gerente de Proyecto y por el Líder de Desarrollo.

El contenido estándar de los temas a incluir en el informe son:

- Avance de las actividades.
- Compromisos pendientes.
- Cambios al proyecto.
- Definición de medidas correctivas.

## **Liberación de Entregables**

### **Documentación**

En cada liberación de software, al final de cada Fase, se entregará la siguiente documentación:

- ✓ Manual de Instalación.
- ✓ Documento de Pruebas Internas.
- ✓ Protocolo de Aceptación.

### **Protocolo de Aceptación**

Previamente a la puesta en marcha de los módulos liberados, es importante realizar una evaluación del mismo en conjunto con el cliente a fin de verificar si se encuentra con las condiciones necesarias para entrar en operación.

Para la ejecución de dicha evaluación se elaborará un Protocolo de Aceptación por el cual se probarán las características indispensables del sistema para su puesta en producción.

### **RIESGOS DETECTADOS**

La evaluación de riesgo identifica situaciones que podrían tener un impacto negativo en los procesos críticos, e intenta cuantificar su gravedad y probabilidad.

El análisis de impacto al negocio ayuda a identificar los procesos más críticos, y describiendo el impacto potencial que tendría una interrupción de esos procesos. Una evaluación de riesgo identifica situaciones internas y externas que podrían tener un impacto negativo en los procesos críticos. También intenta cuantificar la potencial gravedad de tales eventos, y la probabilidad de que ocurran.

Contemplando el proyecto actual, será considerado por parte del gobierno que implementare este nuevo sistema de control de migración de personas, se evaluarán los siguientes riesgos detectables.

- **Información suministrada por el sistema poco precisa**

La robustez y confiabilidad de la información administrada por el sistema para la toma de decisiones, debe ser considerada en forma oportuna, ágil e imparcial, con la posibilidad de efectuar controles online, inspecciones, y/o posteriores auditorías, con informes precisos de usabilidad, cumplimiento de pautas, normas y procedimientos pre-establecidos así como la interpretación adecuada del personal involucrado. La falta de algunas de estas características repercute negativamente en la confiabilidad de la información administrada.

**Impacto:** Alto

**Probabilidad:** Media

- **Comunicaciones electrónicas vulnerables**

Las pautas de seguridad, dada la información sensible contemplada por el sistema de migración, no deberían desentender criterios y protocolos de determinados niveles y jerarquías, necesarios para cada utilidad. Es loable suponer que no cualquier persona debería intercambiar comunicaciones con los puestos fronterizos e inclusive la seguridad física de dichos puestos de labor fronterizos, deberían contemplar protección en forma diferenciada, por ser punto sensible y foco de riesgo a la seguridad de la información operada.

**Impacto:** Medio

**Probabilidad:** Media

- **Controles factibles de ser relajados según intereses puntuales**

Las políticas contempladas en los países que controlan sus fronteras, si bien responden a acuerdos y parámetros impuestos por organismos internacionales, con sus propios controles e imposiciones rutinarias, pueden verse afectadas por criterios dispares entre sus dirigentes, y relajados según interés y/o conveniencia particular de individuos inescrupulosos, en detrimento de la aplicación de la mayoría.

**Impacto:** Medio

**Probabilidad:** Media

- **Poco control de la calidad de desarrollo**

Pruebas insuficientes o dispares con márgenes y resultados distorsionados de procedimientos poco profesionales o con capacidades técnicas diferenciadas, podrían fomentar en principio, una actitud censurable y carga negativa a la implementación del proyecto.

**Impacto:** Medio

**Probabilidad:** Baja

### ADMINISTRACIÓN DE RIESGOS

Una vez que los riesgos para este proyecto han sido identificados –utilizando un análisis táctico, estratégico y operativo– el siguiente paso en un análisis de impacto al negocio es determinar cómo esos riesgos afectan a operaciones específicas del negocio.

Asumamos que si todas las funciones del negocio están llevándose a cabo normalmente, la organización será totalmente viable, competitiva y financieramente sólida.

Si un incidente –interno o externo– afecta negativamente las operaciones del negocio, la organización podría verse comprometida.

### HOJA DE TRABAJO PARA EL ANÁLISIS DE RIESGO

*(Rango de 0.0 a 1.0 para P e I)*

<b>Amenaza</b>	<b>Probabilidad (P)</b>	<b>Impacto (I)</b>	<b>Riesgo = P x I</b>
A.- Información suministrada por el sistema poco precisa	Media = 50 %	Alto = 80 %	Riesgo = 40 %
B.- Comunicaciones electrónicas vulnerables	Media = 40 %	Medio = 60 %	Riesgo = 24 %
C.- Controles factibles de ser relajados según intereses puntuales	Media = 40 %	Medio = 50 %	Riesgo = 20 %
D.- Poco control de la calidad de desarrollo	Baja = 30 %	Medio = 50 %	Riesgo = 15 %

Citando brevemente palabras de la Doctora Schwalbe en su libro Information Technology Project Management: “Un plan de administración de riesgos documenta los procedimientos para administrar el riesgo de un proyecto”. Se entiende que el plan de administración de riesgos es una parte clave en la consecución de un proyecto y puede ser crucial en el desenlace final de éste. Las partes principales, según Schwalbe, que debe incluir son:

- Establecer los responsables de cada tarea concreta que se debe realizar en el proyecto encargado de diseñar un informe de riesgos que puedan suponer dichas tareas.
- Se deben asignar plazos y costo determinado para la realización de tareas que conllevan riesgo.



- También hay que determinar probabilidad e impacto que tienen los distintos riesgos que se están analizando.

Tras conocer los riesgos, hay que elaborar un plan de contención de éstos. Existen distintos planes, distintas estrategias para responder ante los problemas que aparecen en el proyecto:

- Aceptar el riesgo o las consecuencias que este ocasione tras producirse.
- Solventar el riesgo antes de que ocurra eliminando aquella amenaza que le vaya a dar pie o bien transfiriéndoselo a otra empresa subcontratada que se encargue de esa parte.
- Se puede reducir el impacto que ocasione un riesgo o incluso eliminarlo si actúas sobre la actividad que lo vaya a ocasionar y disminuyes la probabilidad de que ocurra.

En el caso de que se pueda llegar a mejorar el proyecto u obtener resultados positivos tras el riesgo, tendremos un plan de respuesta totalmente distinto, destacando las siguientes opciones:

- Asegurar que el riesgo va a ocurrir intentando estimular los factores que vayan a darle lugar.
- Obtener una mayor oportunidad y mejorar el riesgo si se consigue maximizar los factores clave que inducen el riesgo.
- Como en el caso de riesgos negativos, también se puede aceptar el riesgo, compartirlo o cederlo a un tercero si procede.

Considerando estos conceptos, aplicaremos las siguientes respuestas a los riesgos detectados:

#### **A.- Información suministrada por el sistema poco precisa**

El sistema puede estar bien utilizado y ser amigable para los usuarios finales, pero si no presenta la información gerencial requerida en tiempo y forma, no será de utilidad la administración de la información contemplada por el sistema. Por tal motivo deberá efectuarse el relevamiento exhaustivo y contar con el total involucramiento de los altos directivos del área de migración nacional, para identificar cual es la información esperada y acompañar a lo largo del proyecto que dicha presentación evolucione en base a los resultados pretendidos.

## **B.- Comunicaciones electrónicas vulnerables**

Las comunicaciones de los puestos fronterizos con el centro de cómputos central pueden ser vulneradas o interrumpidas. De ser ésta última el sistema deberá contar con mecanismos de control y actualizaciones automatizadas para que la información no operarse online, pueda trabajarse offline y seguir trabajando.

Pero si las comunicaciones son vulneradas, la información sensible puede verse filtrada a personas que tienen malas intenciones para con ellas, o adulterar la información transmitida por dichas comunicaciones, para que algunos controles no sean efectivos a su hora, las mismas deberán contar con un nivel de encriptación avanzado para garantizar su no vulnerabilidad.

## **C.- Controles factibles de ser relajados según intereses puntuales**

Para evitar que los controles contemplados por el proyecto sean relajados de manera voluntaria por los inspectores y supervisores de los puestos fronterizos, se recomienda complementar el actual proyecto con la utilización de cámaras de seguridad y el control regular de ellas.

La simple utilización de las mismas son persuasivas para evitar el uso fraudulento de los controles, de no existir una evidencia de controles regulares de las mismas, deja de ser efectiva, por tal motivo se recomienda complementar el actual proyecto, con cámaras de seguridad visualizando los controles efectuados por los inspectores y supervisores, y su seguimiento por parte de personal de seguridad externo a dichos controles.

## **D.- Poco control de la calidad de desarrollo**

Al ser un sistema experto enfocado en una funcionalidad no muy desarrollada en el mercado, es requerido aplicar política de Quality Assurance profesionales. Si no se dispone de personal calificado en estas prácticas es recomendable buscar asesoramiento y/o participación de consultoras externas que contemplen políticas bien establecidas de calidad de desarrollo de sistemas expertos, complementando dicha participación con la colaboración y comunicación intensiva de los analistas del proyecto y los altos directivos del área de migración nacional.

## Conclusiones

Actualmente a nivel mundial se aprovecha la identificación biométrica de los pasajeros en sus movimientos migratorios, pero no contemplan las características descriptas, que en este proyecto se complementa el análisis de las huellas digitales con el análisis de las venas de las manos (a diferencia de la circunferencia de ellas que se está implementando en algunos países pero no es tan precisa y puede variar dependiendo las circunstancias).

También se complementa el análisis del rostro como consideran muchos países avanzados, con el análisis del iris aprovechando las características del dispositivo elegido y sin invadir la intimidad del pasajero y efectuando un control más exhaustivo, permitiendo registrar dicha característica para futuros controles.

En base a las características tecnológicas descriptas en este proyecto, los avances en los dispositivos biométricos elegidos y la utilización de ellos, se contempla un progreso en la identificación de los individuos sin requerir ahondar en la privacidad o el ámbito íntimo del pasajero.

Como también no solo se registra automáticamente la información contemplada en el documento de identidad presentado, también en base al dispositivo elegido se verifica la validez del mismo mediante técnicas avanzadas de iluminación y el conocimiento de las medidas de seguridad desarrolladas por los diferentes países para garantizar dicha validez, y también verificar dicha información con la información electrónica contemplado en él.

Las ventajas de estas tecnologías elegidas está en que con los mismos dispositivos utilizados para registrar la información básica biométrica, y complementando un poco ellos, se verifica y registra mucha más información biométrica y permite efectuar una identificación más íntegra de la persona, eliminando posibles falsas identificaciones producto de solo contemplar una de éstas características.

Dicho sistema de control de migración, permite complementar los ya existentes controles de movimientos de pasajeros permitiendo brindar información más fidedigna y

mayor información de dichos movimientos, para aportar mejores datos estadísticos y online mediante e-governance, para la toma de decisiones a nivel nacional sobre políticas sociales responsables en su propia población y la extranjera, analizando los movimientos migratorios y cruzarlos con los movimientos de éstos en el territorio nacional.

El proyecto está enfocado en el diseño del módulo contemplando el detalle registrado, permitiendo visualizar todas las alternativas factibles del movimiento, las que ya fueron verificadas por diversos usuarios de puestos de control, pero siempre es bien recibida dicha verificación por parte de la Nación que implementará dicho sistema para adecuar los parámetros allí contemplados, dado que mediante los componentes comunes considerados, ello permite sea customizable a un punto muy detallado.

La plataforma tecnológica, aunque desde el comienzo es sugerida, al igual que las comunicaciones y la administración de software base, no es el enfoque tecnológico aquí desarrollado, siendo el enfoque funcional aplicado al control de movimientos migratorios el que se intenta optimizar mediante este diseño, ofreciendo algunas tecnologías biométricas para un funcionamiento optimizado de la aplicación.

Dado que el avance tecnológico en identificación inequívoca biométrica avanza sin detenerse, y las características biométricas son cada vez más utilizadas por cada vez mayor cantidad de dispositivos de uso hogareño, que las vuelve más vulnerables, es que éstas deben ser complementadas para su uso en el control migratorio, y las características aquí elegidas están lo suficientemente maduras para ser empleadas de manera inédita y todas combinadas en el control de personas.

## Bibliografía

1. *Migración y Seguridad*. **Organización Internacional para las Migraciones**. 2011.
2. **Migraciones, Dirección Nacional de**. Ministerio del Interior y Transporte. 2015.  
<http://www.migraciones.gov.ar/accesible/indexN.php>.
3. **El Instituto médico-legal holandés (NFI)**. *Investigadores crean método para determinar la antigüedad de una huella dactilar*. LA HAYA , 2014.  
<http://www.emol.com/noticias/tecnologia/2014/06/04/663662/investigadores-crean-metodo-para-determinar-la-antigüedad-de-una-huella-dactilar.html>.
4. *Loterías en Supergiros se cobrarán con lector biométrico*. **Portafolio.co**. 2012.
5. *FBI invierte \$1.000 millones en nueva tecnología de reconocimiento facial*. **HispanTV - Nexo Latino**. EE.UU y Canada , 2012.
6. *Sistema de reconocimiento facial 3D*. **Face Recognition and Artificial Vision research laboratory**. Madrid , 2014.
7. *Red de Justicia de Pennsylvania tendrá tecnología de reconocimiento facial*. **ID Noticias** . 2013.
8. *Facebook elimina los datos de reconocimiento facial a los ciudadanos de la UE*. © **DIARIO ABC, S.L.** 2013.
9. *Template Aging Phenomenon in Iris Recognition*. **Biometrics Compendium, IEEE**. 2013.
10. *Hitachi da un paso con firmas digitales biométricas basadas en la vena*. **Planet Biometrics**. 2013.
11. *Una política nacional para el Gobierno electrónico*. **Ibarra, Lito**. 2009.
12. **GOBIERNO ELECTRÓNICO**. **Centro de Investigación y Estudios Avanzados del IPN**. 2010.
13. **(OEA), Organización de los Estados Americanos**. *Sobre e-Gobierno*.
14. **Unidas, Naciones**. Estudio de las Naciones Unidas sobre el Gobierno Electrónico.  
[www.unpan.org/e-government](http://www.unpan.org/e-government). 2012.
15. *Crisis estructurales de ajuste, ciclos económicos y comportamiento de la inversión*. **Pérez, Carlota & Freedman Christopher**. s.l. : Trabajo y Sociedad. 2003, 2013.
16. **Drucker, Peter**. *Escritos fundamentales. La sociedad*. s.l. : Sudamericana, 2012.
17. **David, P. Foray**. *Una introducción a la economía y a la sociedad del saber*. s.l. : Paper 42. UNESCO, 2011.

18. **Weissbluth, Mario.** *Magíster en Gestión y Políticas Públicas, Departamento de Ingeniería Industrial.* 2008.
19. **Fountain, Jane E.** *Building the Virtual State: Information Technology and Institutional Change.* The Brookings Institution , 2011.
20. **Araya Dujisin, R.y Porrúa.** *Casos y tendencias en gobierno electrónico.* Santiago de Chile y OEA , 2014.
21. *Elementos para la creación de una estrategia de gobierno electrónico .* **Vigón, Miguel A. Porrúa.** 2005.
22. *GOBIERNO ELECTRÓNICO: FASES, DIMENSIONES Y ALGUNAS CONSIDERACIONES A TENER EN CUENTA PARA SU IMPLEMENTACIÓN.* **Suárez, Roberto de Armas Urquiza & Alejandro de Armas.** 2011.
23. **Migraciones, OIM Organización Internacional para las.** CONTROL MIGR.   
[http://www.oimperu.org/oim\\_site/documentos/Modulos\\_Fronteras\\_Seguras/](http://www.oimperu.org/oim_site/documentos/Modulos_Fronteras_Seguras/).
24. *Policía de Investigaciones de Chile, Tecnología aplicada al Control Migratorio Aeroportuario.* **Vidal, Raúl Sepúlveda.** 2008.
25. *Acerca de la Biometría - Preguntas Frecuentes.* **Janices, Pedro.** 2012.
26. **Kaspersky Lab.** Los sistemas de verificación biométricos y sus problemas. 2013.   
[http://www.kaspersky.es/about/news/product/2013/Los\\_sistemas\\_de\\_verificacion\\_biometrico\\_s\\_y\\_sus\\_problemas\\_segun\\_Kaspersky\\_Lab\\_](http://www.kaspersky.es/about/news/product/2013/Los_sistemas_de_verificacion_biometrico_s_y_sus_problemas_segun_Kaspersky_Lab_).
27. **Biometrics.gov.** Acerca de la Biometría, Preguntas Frecuentes. 2013.   
<http://www.biometria.gov.ar/acerca-de-la-biometria/preguntas-frecuentes.aspx>.
28. **Micrisoft.** Windows Server Documentation. *Network Load Balance.*   
<https://social.technet.microsoft.com/Forums/windowsserver/es-ES/de679de3-05f4-4fd4-8dfb-17a0e5fe42eb/network-load-balance?forum=windowsserver2008r2highavailability>.
29. *Lector de pasaportes Suprema RealPass - V.* **Kimaldi Electronics, S.L.** 2014.
30. **Klaus Finkenzeller, John Wiley & Sons, Ltd.** *Fundamentals and Applications in Contactless Smart Cards and Identification. Second Edition .* 2013.
31. **Internacional, Organización de Aviación Civil.** *Documentos de viaje de lectura mecánica.* 2006.
32. **Europea, Unión.** Consejos de la Unión Europea, Secretaría General. *REGISTRO PÚBLICO DE DOCUMENTOS AUTÉNTICOS DE IDENTIDAD Y DE VIAJE EN RED.* 2015.
33. **Suprema.** Plataforma de Seguridad Abierta. <https://www.supremainc.com/es/node/133>.

34. **GoIT Chile, Ltda.** Identificación de Huellas Dactilares. *VeriFinger SDK*. 2014.
35. **Biometrics, Fulcrum.** *Iris ID iCAM TD 100 Dual escáner de Iris*. 2012.  
<http://es.fulcrumbiometrics.com/el-es-s17f/Iris-ID-iCAM-TD100-Dual-escaner-de-Iris>.
36. **Authentication™, Advanced Identity.** IrisID.  
<http://www.irisid.com/productssolutions/hardwareproducts/icamtd100/>.
37. **Linda S. Millis, Vice President, Industry Programs, AFCEA International.** About The Biometric Consortium. <http://www.biometrics.org/>. 2015.
38. *Escáner FUJITSU PalmSecure Palma vena.* **Fulcrum Biometrics.** 2014.
39. **Biometricos.NET.** Lector de venas Fujitsu PalmSecure.  
<http://www.biometricos.net/2015/01/lector-de-venas-fujitsu-palmsecure.html>.
40. **Noelia González, Directora de Investigación de Fujitsu.** <http://www.fujitsu.com/es/>.
41. *La seguridad en la palma de la mano.* **González, Noelia.** 2012.
42. *Vasos sanguíneos, nueva clave de seguridad.* **Accogli, Juan Ignacio.** s.l. : InfoBae, 2013.  
<http://www.infobae.com/2013/09/24/1058159-vasos-sanguineos-nueva-clave-seguridad>.
43. **Collazo, Lourdes.** GPS NEWSA. *Revista del Mundo de la Comunicación*. 2014.
44. [http://www.gobierno-digital.gob.mx/wb/gobDigital/gobD\\_GobiernoElectronico](http://www.gobierno-digital.gob.mx/wb/gobDigital/gobD_GobiernoElectronico).  
*Definición del Gobierno electrónico.* 2005.
45. **Linda S. Millis, Vice President, Industry Programs, AFCEA International.** About The Biometric Consortium. <http://www.biometrics.org/>.
46. **Urrutia, Eugenio Rivera.** *Concepto y problemas de la construcción del gobierno electrónico: una revisión de la literatura.* 2006.
47. **K., LAUDON, J.** *Sistemas de informacion gerencial: administracion de la empresa (Octava ed.)*. s.l. : Parson Educación., 2004.
48. **BRISEÑO, GOMEZ DE SILVA y ANIA.** *Sistema de Información.* 2008.
49. **Hernandez, Claudia Marcela.** *Sistemas de información estratégicos.*  
<http://www.grandespymes.com.ar/category/sistemas-de-informacion/>.
50. **Migraciones, OIM Organización Internacional para las.** Control migratorio. *OIM - Misión en el Perú.* 2012. [http://www.oimperu.org/oim\\_site/documentos/Modulos\\_Fronteras\\_Seguras/](http://www.oimperu.org/oim_site/documentos/Modulos_Fronteras_Seguras/).

## ANEXO A

### DESCRIPCIÓN DE LOS COMPONENTES DACTILARES

#### *FingerPrint Matcher*

Compara plantillas biométricas en modos 1-a-1 (verificación) y 1-a-N (identificación). Además incluye un algoritmo fusionado de comparación que permite incrementar la confiabilidad:

- Comparando plantillas que contienen 2 o más registros dactilares (requiere los componentes Segmentar o Client para extraer plantillas desde imágenes que contienen más de una huella);
- Comparando plantillas que contienen registros de huellas, rostros, iris y/o voz (requiere Face Matcher, Iris Matcher y Voice Matcher respectivamente).

El componente Fingerprint Matcher compara 40.000 huellas por segundo y está diseñado para ser usado en sistemas biométricos de escritorio o móviles, que se ejecutan en PC o portátiles con un procesador Intel Core 2 Q9400 de 2,67 GHz.

Se incluye 1 licencia Fingerprint Matcher con VeriFinger 7.1 Standard SDK y VeriFinger 7.1 Extended SDK. Los clientes de VeriFinger 7.1 SDK pueden adquirir más licencias en cualquier momento.

#### *Embedded FingerPrint Matcher*

Posee la misma funcionalidad de Fingerprint Matcher. Compara 3.000 huellas por segundo y puede ser usado en sistemas biométricos integrados o móviles que se ejecuten en dispositivos Android al menos con un procesador Snapdragon S4 (Krait 300 de 4 cores a 1,51 GHz).

Se incluye una licencia Embedded Fingerprint Matcher con VeriFinger 7.1 Standard SDK y VeriFinger 7.1 Extended SDK. Los clientes de VeriFinger 7.1 SDK pueden adquirir más licencias de este componente en cualquier momento.



### *FingerPrint BSS (Biometric Standards Support)*

Permite añadir soporte para plantillas dactilares y formatos de imagen estándar así como formatos adicionales de imagen en sistemas biométricos nuevos o existentes basados en MegaMatcher SDK.

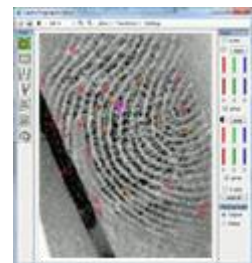
Se soportan los siguientes estándares biométricos:

- BioAPI 2.0 (ISO/IEC 19784-1:2006) (Framework y Biometric Service Provider para el motor de identificación dactilar)
- ISO/IEC 19794-2:2005 (Fingerprint Minutiae Data)
- ISO/IEC 19794-4:2005 (Finger Image Data)
- ANSI/INCITS 378-2004 (Finger Minutiae Format para intercambio de datos)
- ANSI/INCITS 381-2004 (Finger Image-Based Data Interchange Format)
- ANSI/NIST-CSL 1-1993 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- ANSI/NIST-ITL 1a-1997 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- ANSI/NIST-ITL 1-2007 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)
- ANSI/NIST-ITL 1a-2009 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)

El Componente Fingerprint BSS permite la conversión entre plantillas propietarias Neurotechnology, ISO/IEC 19794-2:2005, ANSI/INCITS 378-2004 y plantillas ANSI/NIST-ITL.

El Componente Fingerprint BSS también incluye:

- Módulo de soporte para formato de imagen JPEG 2000 con 1000 ppi Fingerprint Profile;
- Módulo de soporte para formato de imagen NIST IHead;
- Módulo con algoritmo NIST Fingerprint Image Quality (NFIQ), para determinar la calidad de imagen.



Está disponible un Editor de Huellas Latentes con Fingerprint BSS. En muchos casos el procesado automático de imagen es incapaz de extraer todas las minucias o extrae algunos puntos falsos de imágenes latentes (por ejemplo, tomadas de una escena del crimen). Por lo tanto, un experto debe editar manualmente la plantilla dactilar para enviarla a identificación

AFIS. El Editor de ejemplo para huellas latentes (.NET) muestra cómo cambiar las coordenadas de las minucias, dirección, tipo y otros parámetros.

Este componente está diseñado para aplicaciones que se ejecutan en un equipo con un procesador mínimo Intel Core 2 Q9400 a 2,67 GHz. Los clientes de MegaMatcher 5.1 SDK pueden adquirir más licencias de este componente en cualquier momento. Puede usarse desde aplicaciones C/C++, C#, y Java en todas las plataformas soportadas. Se incluyen wrappers .NET de librerías Windows para desarrolladores .NET.

Los clientes de VeriFinger 7.1 Extended SDK pueden adquirir licencias de este componente en cualquier momento.

### *FingerPrint WSQ*

Permite integrar soporte para el formato de imagen WSQ (Wavelet Scalar Quantization) que comprime una imagen dactilar de 10-15 veces. El proceso de compresión WSQ tiene “pérdidas”, por lo que la imagen comprimida no es igual al original (se pierde información). Sin embargo, el algoritmo WSQ fue especialmente diseñado para minimizar la pérdida de información dactilar, así la imagen reconstruida será lo más parecida posible al original.

Nuestra implementación de la compresión de imagen de huellas WSQ 3.1 fue certificada por el FBI por cumplir con los requisitos de precisión en la especificación Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification, Versión 3.1.

Éste componente está diseñado para aplicaciones que se ejecutan en un equipo con un procesador mínimo Intel Core 2 Q9400 a 2,67 GHz. Los clientes MegaMatcher 5.1 SDK pueden adquirir más licencias de éste componente en cualquier momento.

Puede usarse desde aplicaciones C/C++, C#, y Java en todas las plataformas soportadas. Se incluyen wrappers .NET de librerías Windows para desarrolladores .NET.

Los clientes de VeriFinger 7.1 Extended SDK pueden adquirir licencias de este componente en cualquier momento.

### Matching Server

Es un software listo para usar diseñado para construir sistemas web de tamaño moderado y otros sistemas basados en red como AFIS locales o sistemas de identificación multibiométrica. El software Server se ejecuta en un PC servidor y permite realizar la comparación de plantillas biométricas en el servidor usando:

- El componente Fast Fingerprint Matcher o Fingerprint Matcher para la comparación de plantillas de huellas dactilares;
- El componente Fast Face Matcher o Face Matcher para la comparación de plantillas faciales;
- El componente Fast Iris Matcher o Iris Matcher para la comparación de plantillas de Iris.
- El componente Voice Matcher para la comparación de plantillas vocales.

Se puede habilitar la comparación multibiométrica fusionada ejecutando componentes para comparación de huellas, rostros, iris y voz en la misma máquina.

El Módulo de Comunicación del Cliente que permite enviar tareas al Matching Server, consultar el estado de la tarea, obtener resultados y eliminar tareas del servidor, se incluye con MegaMatcher 5.1 SDK, VeriFinger 7.1 SDK, VeriLook 5.6 SDK, VeriSpeak 2.2 SDK y VeriEye 2.9 SDK. Éste módulo oculta todas las comunicaciones de bajo nivel y proporciona un API de alto nivel para el desarrollador.

Los componentes y los módulos de soporte para bases de datos con los códigos fuente incluidos para el componente Matching Server se muestran en la siguiente tabla. El integrador puede desarrollar módulos personalizados para trabajar con otras bases de datos y utilizados con los componentes Matching Server.

El componente Matching Server requiere una licencia especial que permite ejecutar el componente en todas las máquinas que ejecuten los componentes de comparación de huellas, rostros, iris o palma de la mano obtenidos por un integrador. El software Matching Server se incluye con VeriFinger 7.1 Extended SDK.

Además el componente Matching Server se incluye con MegaMatcher 5.1 SDK, VeriLook 5.6 Extended SDK, VeriSpeak 2.2 Extended SDK y VeriEye 2.9 Extended SDK (vea sus catálogos para más detalles).

**RESULTADOS DE LAS PRUEBAS DE CONFIABILIDAD Y DESEMPEÑO**

Presentamos los resultados de las pruebas para mostrar la confiabilidad del algoritmo de comparación de plantillas VeriFinger 7.1 sobre datos de diferentes lectores de huellas dactilares.

Se utilizó una base de datos de huellas planas para realizar las pruebas					
Número de Experimento y descripción de la base de datos		Lector dactilar	Imágenes	Huellas únicas	Tamaño de imagen (píxeles)
1	Base de datos dactilar propietaria 1	DigitalPersona U.are.U 4000	1,400	140	318 x 330
2	Base de datos dactilar propietaria 2	Futronic FS80	1,700	170	320 x 480
3	Base de Datos Dactilar SONATEQ SQ FDB1-75TS1 subconjunto – sólo huellas del dedo índice izquierdo	Cross Match Veri Fier 300 LC	7,500	1,500	640 x 480

Se realizaron 2 pruebas para cada experimento:

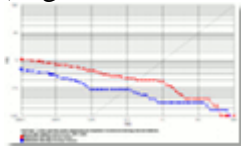
**Prueba 1** maximizando la **precisión**. La confiabilidad de VeriFinger 7.1 se muestra en las **líneas azules** del gráfico ROC.

**Prueba 2** maximizando la **velocidad**. La confiabilidad de VeriFinger 7.1 se muestra en las **líneas rojas** del gráfico ROC.

Las curvas de características de operación del algoritmo (ROC) se utilizan típicamente para graficar la calidad de reconocimiento de un algoritmo. Las curvas ROC muestran la dependencia de la tasa de rechazo falso (FRR) sobre la tasa de reconocimiento falso (FAR).

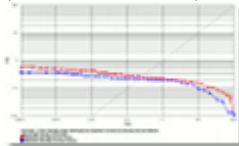
**Experimento 1**

(DigitalPersona U.are.U 4000)



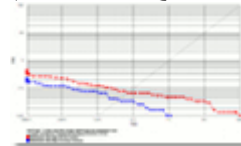
**Experimento 2**

(Futronic FS80)



**Experimento 3**

(SONATEQ FDB1-75TS1)



	Experimento 1		Experimento 2		Experimento 3	
	Prueba 1	Prueba 2	Prueba 1	Prueba 2	Prueba 1	Prueba 2
FRR a 0.01 % FAR	0.096 %	0.461 %	0.288 %	0.438 %	0.074 %	0.130 %
FRR a 0.001 % FAR	0.318 %	0.746 %	0.366 %	0.510 %	0.120 %	0.244 %

Las versiones del algoritmo de identificación de huellas VeriFinger han demostrado consistentemente uno de los mejores resultados de confiabilidad en múltiples competencias biométricas, incluyendo la International Fingerprint Verification Competition (FVC2006, FVC2004, FVC2002 y FVC2000) y la National Institute of Standards & Technology (NIST) Fingerprint Vendor Technology Evaluation (FpVTE 2003), donde VeriFinger se posicionó dentro del Top 5 de precisión en las pruebas individuales.

## ANEXO B

### DESCRIPCIÓN DE LOS COMPONENTES DE IDENTIFICACIÓN DE IRIS PARA SOLUCIONES STAND-ALONE WEB

#### DESCRIPCIÓN DE VERIEYES

La tecnología de identificación de Iris VeriEye está diseñada para desarrolladores e integradores de sistemas biométricos. La tecnología incluye muchas soluciones propietarias que permiten una captura robusta del iris bajo diversas condiciones y comparación rápida en modos 1:1 y 1:N.



VeriEye está disponible como kit de desarrollo de software SDK que permite crear soluciones Stand-alone y para ambiente Web bajo Microsoft Windows, Linux, Mac OSX y Android.

#### VENTAJAS DE VERIEYES

- Identificación rápida y precisa del iris, aprobada por NIST IREX.
- Reconocimiento robusto, incluso si el usuario no está mirando directamente a la cámara o tiene los párpados ligeramente cerrados.
- Algoritmo original propietario que resuelve las limitaciones y obstáculos de los mejores algoritmos actuales.
- Disponible como SDK multiplataforma que soporta diversos lenguajes de programación.
- Precios razonables, licenciamiento flexible y soporte gratuito.
- Resultados sobre un PC con procesador Intel Core 2 Q9400 (2.67 GHz).

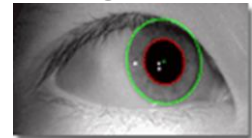
## **CAPACIDADES Y CARACTERÍSTICAS DEL ALGORITMO VERIEYES**

Investigamos y desarrollamos la biometría del iris desde 1994. En 2008, se publicó el algoritmo de reconocimiento de iris VeriEye. Al año siguiente VeriEye fue reconocido por NIST como uno de los algoritmos de reconocimiento de iris más confiables y precisos del mercado.

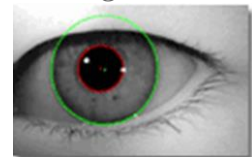
El algoritmo propietario implementa una segmentación avanzada del iris, captura y comparación utilizando técnicas robustas de procesamiento de imágenes digitales:

- **Detección robusta.** Detecta iris aún con obstrucciones en la imagen, ruido visual y/o diferentes niveles de iluminación. Se eliminan obstrucciones por reflejos, párpados y pestañas. También acepta imágenes de ojos entrecerrados y miradas indirectas.
- **Detección automática de entrelazado y corrección** de imágenes de iris en movimiento para plantillas de máxima calidad.
- **Las miradas indirectas** se detectan, segmentan y transforman como si estuvieran viendo directamente a la cámara (ver Figura 1).
- **Correcta segmentación del iris** aún bajo las siguientes condiciones:
  - **No hay círculo perfecto.** Se usan patrones activos de formas que modelan de forma precisa los contornos del ojo cuando los bordes del iris no son círculos perfectos.
  - **El centro, borde interno y borde externo del iris son diferentes** (ver Figura 2). Borde interno y su centro en rojo, borde externo y su centro en verde.
  - **Los bordes del iris no son círculos ni elipses** (ver Figura 3). Especialmente en miradas indirectas.
  - **Los bordes parecen círculos perfectos.** La calidad se puede mejorar si hay bordes precisos (ver Fig. 4) Note las ligeras imperfecciones al comparar con círculos perfectos.
- **Comparación rápida.** La velocidad de comparación es variable y va de 60,000 a 548,000 comparaciones por segundo en un PC. Vea las especificaciones técnicas para más detalles.

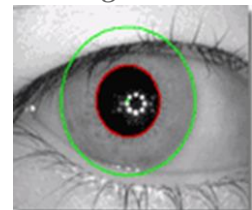
*Figura 1*



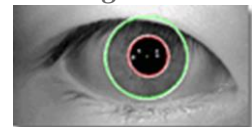
*Figura 2*



*Figura 3*



*Figura 4*



- **Confiabilidad.** VeriEye 2.9 muestra un excelente desempeño cuando se pone a prueba con los conjuntos de datos disponibles públicamente. Conseguimos resultados especialmente buenos con la reciente base de datos NIST ICE2005 Exp1 con imágenes de iris de calidad intencionalmente disminuida (vea la sección de Resultados de las Pruebas de Confiabilidad y Desempeño).

Todas las imágenes pertenecen a la Base de Datos CASIA Iris V2.0 y CASIA Iris V3.0 del Instituto de Automatización de la Academia China de Ciencias (CASIA)

## DESCRIPCIONES DE COMPONENTES BIOMÉTRICOS

### *Iris Matcher*

Realiza la comparación de plantillas en modos in 1:1 (verificación) y 1:N (identificación) sobre PC o Mac. Además incluye un algoritmo fusionado que permite aumentar la confiabilidad de la comparación al:

- Comparar plantillas que contienen 2 registros de iris;
- Comparar plantillas que contienen huellas, rostros, voz y/o iris (la comparación de huellas, rostros y voz requiere los componentes Fingerprint Matcher, Face Matcher y Voice Matcher respectivamente – vea los catálogos VeriFinger SDK, VeriLook SDK y VeriSpeak SDK para más detalles);

El componente Iris Matcher compra 40,000 iris por segundo y se usa en sistemas biométricos móviles o de escritorio, en PC o portátiles con procesador mínimo Intel Core 2 Q9400 (2.67 GHz).

Se incluye una licencia Iris Matcher con VeriEye 2.9 Standard SDK y VeriEye 2.9 Extended SDK. Los clientes de VeriEye 2.9 SDK pueden adquirir más licencias de este componente en cualquier momento.



### *Embedded Iris Matcher*

Posee la misma funcionalidad que Iris Matcher. Compara 3,000 iris por segundo y está diseñado para usarse en sistemas biométricos incrustados móviles, en dispositivos Android con procesador Snapdragon S4 (Krait 300 de 4 núcleos a 1.51 GHz) o superior.

Se incluye una licencia Embedded Iris Matcher con VeriEye 2.9 Standard SDK y VeriEye 2.9 Extended SDK. Los clientes de VeriEye 2.9 SDK pueden adquirir más licencias de este componente en cualquier momento.

### *Iris BSS (Biometric Standards Support)*

El componente Iris BSS (Biometric Standards Support) permite añadir soporte para formatos estándar de iris y formatos adicionales de imagen a sistemas biométricos nuevos o existentes basados en VeriEye SDK.

Soporta los siguientes estándares biométricos:

- BioAPI 2.0 (ISO/IEC 19784-1:2006) (Framework y Biometric Service Provider para motores de identificación de iris)
- ISO/IEC 19794-6:2005 (Iris Image Data)
- ANSI/INCITS 379-2004 (Formato de Intercambio de Imágenes de Iris)

El componente está diseñado para aplicaciones que se ejecutan en un procesador mínimo Intel Core 2 Q9400 (2.67 GHz). Puede ser usado en aplicaciones C/C++, C# y Java sobre todas las plataformas compatibles. Se proporcionan .NET wrappers de librerías Windows para desarrolladores .NET.

Los clientes de VeriEye 2.9 SDK pueden adquirir más licencias de este componente en cualquier momento.

### *Matching Server*

Es un software listo para usar ideal para construir sistemas de tamaño moderado basados en Web y Redes como aplicaciones de identificación simple o multibiométrica. Se ejecuta en un PC servidor y permite realizar la comparación de plantillas biométricas en el lado del servidor usando el componente Iris Matcher.

La comparación multibiométrica se puede habilitar ejecutando componentes de verificación de iris, huellas, rostros y voz en el mismo equipo.

El módulo de comunicación del cliente que permite enviar tareas al Servidor de Comparación, consultar el estado de las tareas, obtener los resultados y eliminar tareas del servidor, se incluye con MegaMatcher 5.1 SDK, VeriFinger 7.1 SDK, VeriLook 5.6 SDK, VeriSpeak 2.2 SDK y VeriEye 2.9 SDK. Este módulo oculta todas las comunicaciones de bajo nivel y proporciona un API de alto nivel para el programador.

### **RESULTADOS DE LAS PRUEBAS DE CONFIABILIDAD**

Presentamos los resultados de las pruebas para comprobar la confiabilidad del algoritmo de comparación de plantillas VeriEye 2.9. Se utilizaron imágenes de iris de diversas bases de datos estándar para las pruebas, y así poder comparar los resultados con otros algoritmos. Todas las bases de datos contienen imágenes de iris de tamaño 640 x 480 píxeles.

<b>Bases de Datos de imágenes de iris usadas para probar el algoritmo VeriEye 2.9</b>			
<b>Nombre de la Base de Datos</b>	<b>Cantidad de imágenes</b>	<b>Cantidad de Personas</b>	<b>Cantidad de ojos únicos</b>
<b>ICE2005 Exp1 (Iris Derecho)</b>	1,425	124	124
<b>Universidad de Notre Dame, ND-IRIS-0405</b>	64,980	356	712
<b>Universidad de Bath, IRISDB1600 <sup>(1)</sup></b>	24,361	624	1231

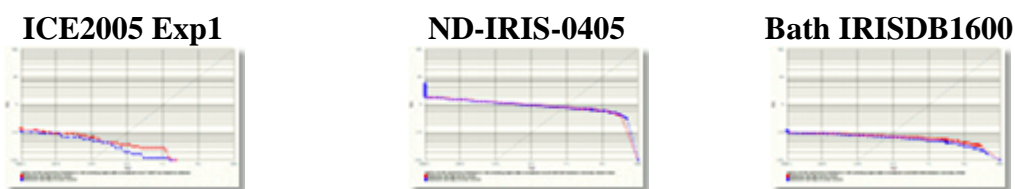
(1) La base de datos completa IRISDB1600 contiene 31,997 imágenes (tamaño 1280x960 píxeles), que representan 799 personas únicas y 1,598 iris únicos. Fue pre procesado un subconjunto utilizado en esta prueba similar a los experimentos NIST IREX:

- (a) Las imágenes fueron reducidas a 640x480 vía promediado 2x2.
- (b) Todas las imágenes con iris de diámetros mayores a 340 fueron eliminadas.

Se realizaron dos pruebas con cada base de datos:

- Prueba 1. Máxima precisión de reconocimiento. La confiabilidad del algoritmo VeriEye 2.9 en esta prueba se muestra en las líneas azules en la gráfica de curvas ROC.
- Prueba 2. Velocidad maximizada. La confiabilidad del algoritmo VeriEye 2.9 en esta prueba se muestra en las líneas rojas en la gráfica de curvas ROC.

La tolerancia de rotación del iris fue establecida en  $\pm 15^\circ$  para todas las pruebas. Las curvas de Características de Operación del Receptor (ROC) típicamente se utilizan para demostrar la calidad de reconocimiento de un algoritmo. Las curvas ROC muestran la dependencia de la Tasa de Falso Rechazo (FRR) sobre la Tasa de Falsa Aceptación (FAR).



<b>Resultados de las pruebas de confiabilidad del algoritmo VeriEye 2.9, FRR a 0.001 % FAR</b>		
	<b>Prueba 1</b>	<b>Prueba 2</b>
<b>Base de Datos ICE2005 Exp1</b>	0.0983 %	0.1187 %
<b>Base de Datos ND-IRIS-0405</b>	1.5550 %	1.6000 %
<b>Base de Datos BATH IRISDB1600</b>	0.0893 %	0.0928 %

## ANEXO C

### IDENTIFICACIÓN DE ROSTROS PARA SISTEMAS STAND- ALONE Y APLICACIONES PARA AMBIENTE WEB

La tecnología de identificación facial VeriLook está diseñada para desarrolladores e integradores de sistemas biométricos. Proporciona un gran desempeño y confiabilidad con detección de rostro vivo, reconocimiento simultáneo de múltiples rostros y rápida comparación en modos 1:1 y 1:N.

VeriLook está disponible como SDK que permite el desarrollo de soluciones para ambientes PC y Web bajo Microsoft Windows, Linux, Mac OS X y Android.

#### *Ventajas de VeriLook*

- Más de un millón de soluciones alrededor del mundo utilizan VeriLook.
- Detección de “rostro vivo” evita fraudes colocando una foto frente a la cámara.
- Procesado simultáneo de múltiples rostros en video y fotografías.
- Clasificación de géneros y extracción de puntos faciales característicos de cada persona en una imagen.
- Se pueden utilizar Webcams u otras cámaras de bajo costo.
- Disponible como SDK multiplataforma compatible con diversos lenguajes de programación.
- Disponible SDK de vigilancia para integrar en sistemas de seguridad.
- Precios razonables, licenciamiento flexible y soporte gratuito.

#### **IDENTIFICACIÓN FACIAL**

Actualmente existen muchos tipos de identificación biométrica: huellas, Iris, retina, voz, rostros, etc. Cada uno de esos métodos tiene ventajas y desventajas que se deben considerar al desarrollar sistemas biométricos, tales como: confiabilidad del sistema, precio, flexibilidad, necesidad de contacto físico con que el dispositivo de captura y muchos otros. Seleccionar cierto método de identificación biométrica o utilizar un sistema multi biométrico puede ayudar a soportar esos requerimientos generalmente discrepantes.

El reconocimiento de rostros puede ser una alternativa importante para seleccionar y desarrollar un sistema biométrico óptimo. Su ventaja es que no requiere contacto físico con el

dispositivo de captura de imágenes (cámara). Un sistema de identificación facial no requiere hardware avanzado, porque puede ser utilizado con dispositivos existentes de captura de imagen (Webcams, cámaras de seguridad, etc.)

Por lo tanto, el reconocimiento facial debe ser considerado como una alternativa seria en el desarrollo de sistemas biométricos o multi biométrica.

### **TECNOLOGÍA DE RECONOCIMIENTO FACIAL**

Tal como la biometría dactilar, la tecnología de reconocimiento facial es ampliamente usada en diversos sistemas, incluyendo control de acceso y seguridad de cuentas computarizadas.

Usualmente esos sistemas extraen ciertas características de la imagen de un rostro y realizan la comparación utilizando esas características. Un rostro no posee tantas características únicas comparables como las huellas dactilares o el iris, por lo tanto el reconocimiento facial es ligeramente menos confiable que otros métodos de reconocimiento biométrico. Sin embargo, sigue siendo apropiado para muchas aplicaciones, especialmente cuando se toma en cuenta la comodidad y conveniencia para el usuario. El reconocimiento facial también puede ser utilizado junto con el reconocimiento dactilar u otro método biométrico para desarrollar aplicaciones donde la seguridad es crítica.

El enfoque multi biométrico es especialmente importante para sistemas de identificación (1:N). En general, los sistemas de identificación son muy convenientes de usar porque no requieren información adicional de seguridad (tarjetas inteligentes, contraseñas, etc.). Sin embargo, utilizar rutinas de identificación 1:N con un solo método biométrico, puede arrojar una alta tasa de aceptación falsa, lo que sería inaceptable en aplicaciones con grandes bases de datos. Utilizar la identificación facial como un método biométrico adicional puede disminuir dramáticamente este efecto.

Este enfoque multibiométrico también es útil en situaciones donde determinada característica biométrica no es óptima para un grupo de usuarios. Por ejemplo, las personas que realizan trabajo pesado con sus manos pueden tener huellas dactilares ásperas, lo que aumenta la tasa de falso rechazo en caso de utilizar únicamente identificación dactilar.

## CAPACIDADES Y CARACTERÍSTICAS DEL ALGORITMO VERILOOK

VeriLook localiza, almacena y compara rostros utilizando algoritmos avanzados para procesamientos de imágenes digitales:



- **Procesado simultáneo de múltiples rostros.** VeriLook 5.6 realiza una rápida y precisa detección de múltiples rostros en **videos** e imágenes. Todos los rostros se detectan en **0.01 - 0.86 segundos** según configuración. De cada rostro se **extraen** sus características en **0.6 segundos** y se almacenan en una plantilla biométrica. Vea las especificaciones técnicas para más detalles.
- **Clasificación de Género.** Opcionalmente, Se puede determinar el género de cada persona con un margen predefinido de precisión.
- **Detección de rostro vivo.** Un sistema convencional de identificación de rostros puede ser engañado colocando una foto frente a la cámara. VeriLook puede evitar este fallo de seguridad determinando si el rostro está “vivo” o es una foto. Vea las recomendaciones para detección de rostro vivo para obtener más detalles.
- **Reconocimiento de Emociones.** VeriLook puede detectar rabia, disgusto, miedo, felicidad, tristeza y sorpresa indicando la intensidad de la expresión.
- **Puntos Característicos Faciales.** Opcionalmente se puede extraer un conjunto de coordenadas del rostro. Cada punto característico posee un número secuencial predefinido (ej. El número 67 siempre corresponde a la punta de la nariz).
- **Atributos faciales.** VeriLook puede ser configurado para detectar ciertos atributos durante la extracción – **sonrisa, boca abierta, ojos cerrados, gafas de visión y de sol.**
- **Filtro de calidad de imagen.** Se puede utilizar un filtro durante la captura para garantizar que sólo se almacenen en base de datos imágenes de alta calidad.
- **Tolerancia de posición.** VeriLook permite 360 grados de rotación. El giro de la cabeza puede ser de hasta 15° en cada dirección desde la posición frontal. La inclinación puede ser de hasta 45° en cada dirección. Vea las especificaciones técnicas para más detalles.

- **Múltiples muestras del mismo rostro.** Una plantilla biométrica puede contener varias muestras de la misma persona capturadas de varias fuentes y en distintas oportunidades, permitiendo mejorar la calidad del reconocimiento. Por ejemplo, una persona se puede inscribir con lentes y sin ellos, o con diferentes tipos de lentes; con y sin barba, bigote, etc.
- **Capacidad de Identificación.** VeriLook puede verificar **1:1**, e identificar **1:N** hasta **40,000 rostros**
- **por segundo** en un PC. Vea las especificaciones técnicas para más detalles.
- **Registros pequeños.** Una plantilla puede ser de sólo **4 Kilobytes**, y se pueden utilizar grandes bases de datos. Se puede aumentar el tamaño de la plantilla para mejorar la precisión. Vea las especificaciones técnicas para más detalles.
- **Generalización de características.** Esta función genera una colección de características a partir de varias imágenes de la misma persona que se almacenan en una sola plantilla para mejorar considerablemente la calidad del reconocimiento.

### **CONTENIDO DE VERILOOK 5.6 STANDARD SDK Y EXTENDED SDK**

VeriLook SDK permite desarrollar rápidamente aplicaciones biométricas garantizando una identificación de rostros rápida y confiable. Se puede integrar fácilmente en un sistema de seguridad. Proporciona completo control sobre los datos de entrada y salida del SDK.

VeriLook SDK incluye una Librería de Administración de Dispositivos que **permite capturar imágenes de múltiples cámaras** y también desarrollar **plugins para soportar otras cámaras**:

- VeriLook 5.6 Standard SDK permite crear aplicaciones biométricas para PC, y móviles. Incluye ejemplos de programación, tutoriales, una Librería de Administración de Dispositivos y documentación. Compatible con Microsoft Windows, Linux, Mac OS X y Android.
- VeriLook 5.6 Extended SDK permite crear aplicaciones biométricas para ambiente Web y de redes. Incluye el Standard SDK, clientes para PC y dispositivos Android, aplicaciones cliente de ejemplo, tutoriales y un servidor de comparación listo para usar.

## DESCRIPCIÓN DE LOS COMPONENTES BIOMÉTRICOS

### *Face Matcher*

Realiza la comparación de plantillas faciales en los modos 1:1 (verificación) y 1:N (identificación). Además el componente Face Matcher incluye un algoritmo fusionado de comparación que permite aumentar la confiabilidad de los resultados comparando plantillas que contienen registros de huellas, rostros, voz y/o iris (note que la comparación de huellas, iris y voz requiere adquirir licencias de los componentes Fingerprint Matcher, Iris Matcher y Voice Matcher respectivamente).

El componente Face Matcher compara **40,000 rostros** por segundo y está diseñado para ser usado en sistemas biométricos de **escritorio** o **móviles**, que se ejecuten en un **PC** o **laptop** con procesador al menos Intel **Core 2 Q9400** (2.67 GHz).

Se incluye una licencia Face Matcher con VeriLook 5.6 Standard SDK, VeriLook 5.6 Extended SDK, MegaMatcher 5.1 Standard SDK y MegaMatcher 5.1 Extended SDK. Los clientes VeriLook 5.6 SDK y MegaMatcher 5.1 SDK pueden adquirir más licencias en cualquier momento.

### *Embedded Face Matcher*

Posee la misma funcionalidad del componente Face Matcher. Compara **3,000 rostros por segundo** y está diseñado para usarse en sistemas biométricos **integrados** o **móviles** de dispositivos **Android** basados un procesador al menos **Snapdragon S4 (Krait 300** con 4 cores @ 1.51 GHz).

Se incluye una licencia Embedded Face Matcher con VeriLook 5.6 Standard SDK, VeriLook 5.6 Extended SDK, MegaMatcher 5.1 Standard SDK y MegaMatcher 5.1 Extended SDK. Los clientes VeriLook 5.6 SDK y MegaMatcher 5.1 SDK pueden adquirir más licencias en cualquier momento.



### *Face BSS (Biometric Standards Support)*

Permite añadir soporte para formatos estándar de imagen facial y formatos adicionales de imagen en sistemas biométricos nuevos o existentes basados en MegaMatcher SDK. Están soportados los siguientes estándares biométricos:

- **BioAPI 2.0 (ISO/IEC 19784-1:2006)** (Framework and Biometric Service Provider for Face Identification Engine)
- **CBEFF** (Common Biometric Exchange Formats Framework)
- **ISO/IEC 19794-5:2005** (Face Image Data)
- **ISO/IEC 19794-5:2011** (Face Image Data)
- **ANSI/INCITS 385-2004** (Face Recognition Format for Data Interchange)
- **ANSI/NIST-CSL 1-1993** (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- **ANSI/NIST-ITL 1a-1997** (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- **ANSI/NIST-ITL 1-2000** (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- **ANSI/NIST-ITL 1-2007** (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)
- **ANSI/NIST-ITL 1a-2009** (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)

El componente Face BSS también permite integrar **JPEG 2000** con soporte de Perfil Facial con y sin pérdida en aplicaciones basadas en MegaMatcher SDK.

El componente está diseñado para aplicaciones que se ejecuten sobre un hardware con procesador al menos Intel **Core 2 Q9400** (2.67 GHz).

Los clientes VeriLook 5.6 Extended SDK y MegaMatcher 5.1 SDK pueden adquirir licencias de este componente en cualquier momento.

### **RECOMENDACIONES BÁSICAS PARA IDENTIFICACIÓN DE ROSTROS**

La precisión del reconocimiento facial de VeriLook depende altamente de la calidad de la imagen. **La calidad durante la captura es importante**, porque incide sobre la plantilla biométrica.

Estas son recomendaciones básicas y restricciones al usar aplicaciones de reconocimiento facial basadas en VeriLook SDK.

### *Cámaras e imágenes*

1. Se recomienda utilizar **cámaras de calidad similar** tanto para la captura como para la identificación. Utilizar el mismo modelo de cámara sería mucho mejor.
2. **50 píxeles de distancia mínima recomendada entre los ojos** para realizar correctamente la extracción de plantillas. Se recomiendan **75 píxeles o más** para mejores resultados. Esta distancia debe ser **nativa**, no alcanzada aumentando la imagen.
3. Resolución mínima de cámara **640 x 480 píxeles** para captura y reconocimiento:
  1. Asegúrese de que la resolución **nativa** sea de 640 x 480 en la Webcam o cámara de Smartphone, porque algunas de estas cámaras tienen una resolución más baja que aumentan hasta 640 x 480 sin mejorar la calidad de la foto. Esto es aceptable para video llamadas o fotografía ocasional, pero distorsiona una imagen facial.
  2. No se recomiendan cámaras de una resolución inferior porque las distorsiones ópticas afectarán la calidad de la plantilla biométrica ya que el usuario debe estar demasiado cerca de la cámara para una detección y registro exitoso.
4. **No utilice imágenes reflejo**, El reconocimiento fallará si se utilizan imágenes reflejo para la captura y se intenta luego identificar una imagen nativa (efecto espejo), o viceversa. Algunas cámaras se configuran para producir imágenes con efecto espejo o lo hacen de forma predeterminada. Recomendamos el uso de imágenes con orientación uniforme – todas las imágenes deben ser nativas o reflejadas pero no una mezcla de ambos tipos.
5. **Utilice varias imágenes en la captura**, para aumentar la calidad y confiabilidad.

### *Iluminación*

Se recomienda controlar las condiciones de luz:

- **Luz frontal directa o difundida** permite una distribución equitativa a ambos lados del rostro, arriba y abajo evitando sombras.
- **Evite el brillo** en la piel del rostro, vidrios, lentes y reflejos solares u otra fuente de luz.

### *Postura del Rostro*

El motor de reconocimiento facial tiene cierta tolerancia a la postura del rostro:

1. • **Rotación** de la cabeza –  $\pm 180$  grados (configurable);
  1. El valor predeterminado de  $\pm 15$  grados es la configuración más rápida y usualmente es suficiente para la mayoría de las imágenes frontales del rostro.
2. • **Giro** de la cabeza –  $\pm 15$  grados de la posición frontal.
  1. La tolerancia se puede aumentar hasta  $\pm 25$  grados si la plantilla biométrica creada durante la captura contiene diferentes ángulos.
3. • **Inclinación** de la cabeza –  $\pm 45$  grados de la posición frontal (configurable).
  1. El valor **predeterminado de  $\pm 15$  grados** es la configuración más rápida y usualmente es suficiente para la mayoría de las imágenes frontales del rostro.
  2.  **$30^\circ$  de diferencia** entre la plantilla y el rostro frente a la cámara es aceptable.
  3. Se pueden ingresar varias vistas del mismo rostro para cubrir hasta  $\pm 45$  grados.

### *Expresión Facial*

Se recomienda una **Expresión Neutral del rostro durante la captura**, una expresión no neutral afecta la precisión. Ejemplos de expresiones no neutrales (permitidas pero no recomendadas):

- Amplia sonrisa (exposición de los dientes o el interior de la boca).
- Cejas levantadas (asombro).
- Ojos cerrados.
- Ojos mirando lejos de la cámara.
- Ceño fruncido.

**Ligeros cambios en la expresión facial son aceptables para identificar**, porque no influyen en la precisión del reconocimiento.

### *Expresión Facial*

Se requiere un flujo de imágenes consecutivas (usualmente vídeo de una cámara) para comprobación de vida:

1. Se requieren al menos **10 cuadros**. Se recomiendan 10 – 25 cuadros.
2. Sólo **un rostro visible** en esos cuadros.
3. Cuando se active esta verificación, se realiza **automáticamente** durante la extracción. Si el rostro en el video **no** califica como "vivo", **no se extrae** la plantilla.
4. La detección puede **mejorar** al realizar las siguientes acciones (juntas o por separado):
  1. Mover la cabeza un poco;
  2. Inclinar el rostro;
  3. Alejarse y acercarse a la cámara;
  4. Cambiar ligeramente la expresión facial.

Por ejemplo, el usuario puede comenzar con la cabeza inclinada ligeramente a la izquierda y moverla lentamente hacia la derecha mientras cambia ligeramente la expresión facial (sin dejar de ser visible para la cámara)

### *Lentes, Maquillaje, Cabello, Barba y Bigote*

Se recomiendan varias imágenes con variaciones de apariencia para garantizar la calidad del reconocimiento en situaciones cuando parte de la cara se cubre con lentes o cabello:

1. Lentes – capturas separadas con y sin lentes garantiza una mejor calidad de reconocimiento en ambos casos. Recomendaciones especiales:
  1. Lentes de sol y lentes regulares de marco grande disminuyen la calidad porque cubren parte del rostro. Si es posible, se deben evitar para captura e identificación.
  2. Lentes de Contacto – No afectan el reconocimiento. Sin embargo, quienes los usan algunas veces pueden usar anteojos regulares, en lugar de sus lentes de contacto. En este caso se recomienda un registro usando anteojos convencionales.
2. No se recomienda un maquillaje recargado porque oculta o distorsiona características.
3. Peinados – algunos peinados pueden cubrir parte del rostro, por lo que se recomienda el uso de ganchos de pelo durante la captura y reconocimiento.
4. Cambios en el estilo de vello facial podrían requerir enrolamiento adicional, especialmente cuando crece la barba o el bigote o después de una rasurada.

## PRUEBAS DE CONFIABILIDAD Y RENDIMIENTO

Presentamos los resultados de las pruebas para mostrar la confiabilidad del algoritmo de comparación de plantillas faciales VeriLook 5.6. Se utilizaron imágenes de rostros de la base de datos FRGC para realizar las pruebas, por lo que los resultados pueden compararse con los de otros algoritmos.

**El Experimento 1** y el **Experimento 2** se llevaron a cabo de acuerdo al protocolo FRGC:

- **Experimento 1** mide el desempeño del reconocimiento sobre imágenes frontales de rostros tomadas bajo iluminación controlada. Las muestras biométricas en los conjuntos objetivo y de consulta, consisten de una **fotografía individual controlada** en alta resolución.
- **Experimento 2** está diseñado para examinar el efecto que tienen múltiples fotografías en el desempeño. Las muestras biométricas en los conjuntos objetivo y de consulta, están compuestas de **4 imágenes controladas** de una misma persona.
- Revise el resumen de FRGC para más detalles sobre el protocolo de los experimentos FRGC.

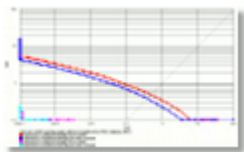
Cada experimento se realizó 2 veces para probas distintos escenarios:

- **Prueba 1 precisión maximizada.** Los resultados de esta prueba se muestran en el gráfico ROC como las curvas **azules** para el Experimento 1 y **cian** para el Experimento 2.
- **Prueba 2 tamaño mínimo de plantilla.** Los resultados de esta prueba se muestran en el gráfico ROC como las curvas **rojas** para el Experimento 1 y **magenta** para el Experimento 2.

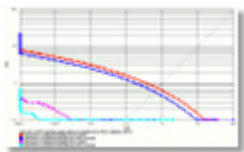
Los conjuntos de curvas ROC fueron calculados usando ciertos subconjuntos de la base de datos FRGC para cada experimento y prueba de acuerdo al protocolo FRGC:

- **ROC I** – las fotos de la galería fueron tomadas durante 6 meses.
- **ROC II** – las fotos de la galería fueron tomadas durante 1 año.
- **ROC III** – las fotos de la galería fueron tomadas durante un lapso de al menos 6 meses pero dentro de 1 año y medio.

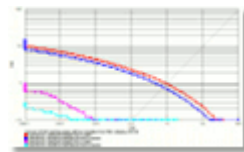
**ROC**



**I ROC**



**II ROC**



**III**

*Notas:*

- Parte de las imágenes de la base de datos FRGC es de 1600 x 1200 pixeles, y la otra parte es de 2272 x 1704 pixeles, porque las imágenes se obtuvieron con una cámara digital. Las especificaciones técnicas están dadas para imágenes de 640 x 480 pixeles que es la resolución tradicional de webcams.
- La tolerancia de giro, inclinación y rotación se estableció en  $\pm 15^\circ$  para todos los experimentos y pruebas.
- No se utilizaron técnicas de normalización de puntuación para calcular las curvas ROC, aunque el protocolo FRGC permitía la aplicación de esta técnica.

**Resultados de las pruebas del algoritmo VeriLook 5.6 con la Base de Datos FRGC**

		Experimento 1		Experimento 2	
		Prueba 1	Prueba 2	Prueba 1	Prueba 2
<b>FRR a 0.1 % FAR</b>	<b>ROC I</b>	0.7107 %	0.9064 %	0.0000 %	0.0000 %
	<b>ROC II</b>	1.2680 %	1.6450 %	0.0087 %	0.0173 %
	<b>ROC III</b>	1.8350 %	2.3410 %	0.0185 %	0.0185 %

## ANEXO D

### IDENTIFICACIÓN AFIS Y MULTIBIOMÉTRICA PARA PROYECTOS DE GRAN ESCALA

#### DESCRIPCIÓN DE MEGAMATCHER

La tecnología MegaMatcher está diseñada para desarrolladores de sistemas multibiométricos y AFIS de gran escala. La tecnología garantiza alta confiabilidad y gran velocidad de identificación biométrica incluso en grandes bases de datos.

MegaMatcher está disponible como Kit de Desarrollo de Software que permite la creación de productos de gran escala biométricos o multibiométricos de huellas dactilares, rostros, iris, voz y la palma de la mano, para las plataformas Microsoft Windows, Linux, Mac OS X y Android.

#### VENTAJAS DE MEGAMATCHER

- Probado en proyectos de escala nacional, incluyendo emisión de pasaportes y comicios electorales.
- Motor dactilar compatible con NIST MINEX
- Motor de iris compatible con NIST IREX.
- Puede comparar 200,000,000 de iris o 100,000,000 de huellas o rostros por segundo con MegaMatcher Accelerator.
- Se pueden comparar huellas, iris y rostros en tarjetas inteligentes utilizando MegaMatcher On Card.
- Incluye modalidad dactilar, facial, vocal, ocular y de palma de la mano.
- Comparación de huellas roladas, planas y latentes.
- Soporte de BioAPI 2.0 y otros estándares biométricos ANSI e ISO.
- Arquitectura de clúster multiplataforma, escalable para comparación en paralelo.
- Efectiva relación precio/desempeño, licenciamiento flexible y soporte gratuito.

## UTILIZADES DE SISTEMAS BOMÉTRICOS DE GRAN ESCALA

Hoy en día, la necesidad de sistemas automatizados de identificación biométrica está aumentando en campos de aplicación civil y forense. Una identificación rápida y precisa se vuelve particularmente crítica para aplicaciones de gran alcance, como documentación de pasaportes y visas, control de fronteras y aduanas, registro de votantes y supervisión de sistemas electorales, control de transacciones con tarjetas de débito y crédito e investigaciones criminales. Muchos países, incluyendo los Estados Unidos, países europeos y otros, incorporan datos biométricos en pasaportes, documentos de identificación, visas y otros para su uso en sistemas de identificación biométrica implementados a nivel nacional.



Los Sistemas Automatizados de Identificación Dactilar (AFIS) han sido ampliamente usados en aplicaciones forenses durante las últimas dos décadas, y recientemente se han vuelto también **relevantes para aplicaciones civiles**. Las aplicaciones biométricas de gran escala requieren ser altamente confiables y veloces. Los sistemas multibiométricos que incorporan reconocimiento de rostros, huellas, iris y/o reconocimiento de voz, ahora también pueden proporcionar estas características y muchas otras ventajas como una mejorada calidad de identificación y versatilidad.

Los sistemas automáticos de identificación biométrica de gran escala tienen requerimientos especiales diferentes de los sistemas biométricos de pequeño o mediano alcance:

- El sistema debe realizar una identificación confiable con grandes bases de datos. Los sistemas de identificación biométrica tienden a acumular una tasa de aceptación falsa a medida que incrementa el tamaño de la base de datos y el uso de un solo patrón biométrico como la huella, el rostro o el Iris puede resultar poco confiable en aplicaciones de gran alcance. Utilizar varias imágenes dactilares de los diferentes dedos de una persona o registrar ambos Iris aumentará la confiabilidad de la comparación. Las tecnologías multi biométricas (por ejemplo: capturar muestras de huellas, rostros y/o Iris de una persona) aumentarán aún más la confiabilidad. Un algoritmo **fusionado** se utiliza para crear una única decisión de identificación basada en los resultados de esas múltiples comparaciones.



- El sistema debe tener una alta productividad y eficiencia, sin importar el tamaño:
  - La escalabilidad del sistema es importante, porque un sistema puede continuar expandiéndose, la base de datos continuará creciendo y debe ser posible mantener la productividad en un alto nivel simplemente añadiendo nuevas unidades al sistema existente.
  - El número diario de peticiones de identificación puede ser muy alto para ciertas aplicaciones.
  - Las peticiones deben ser procesadas de la forma más rápida y eficiente posible (idealmente en tiempo real), lo que demanda un poder computacional de procesamiento considerable.
  - Frecuentemente se requiere soportar grandes bases de datos (decenas o cientos de millones de registros).
  - El sistema debe ser generalmente robusto y tolerante a fallas hardware, porque interrupciones temporales pueden causar problemas y comprometer a todo el sistema en aplicaciones de gran escala.
- El sistema debe soportar la mayoría de los estándares biométricos, permitiendo así el uso de plantillas genéticas o bases de datos dentro de una variedad de plataformas, independientemente del fabricante.
- El sistema debe ser capaz de comparar huellas dactilares planas contra huellas roladas porque muchas instituciones poseen bases de datos de huellas roladas.
- El sistema debe ser capaz de trabajar en red porque en la mayoría de los casos las estaciones cliente se encuentran en ubicaciones remotas lejos del servidor central y la base de datos.
- Un sistema forense debe ser capaz de editar plantillas de huellas latentes que luego serán procesadas en sistemas de identificación AFIS.

Además de estas características, el precio del sistema debe ser lo más bajo posible.

Los sistemas AFIS existentes, muchos de los cuales fueron desarrollados específicamente para aplicaciones de criminalística u otras áreas especializadas, por lo general son bastante costosas. MegaMatcher incluye tecnología y soluciones para productos de gran escala para identificación AFIS o multi biométrico de huellas, Iris, rostros, voz y palma de la mano. MegaMatcher cumple con todas las características mencionadas anteriormente a un precio competitivo.

## CAPACIDADES Y CARACTERÍSTICAS DEL ALGORITMO MEGAMATCHER

MegaMatcher incluye motores de reconocimiento de huellas, rostros, voz, iris y palma de la mano, junto con un nuevo algoritmo fusionado para una identificación rápida y confiable en sistemas de gran escala.

Los algoritmos de identificación dactilar, facial, vocal y ocular pueden ser usados por separado para desarrollar sistemas de identificación automática AFIS, de rostro, de voz o de iris de forma independiente.

Los motores biométricos contienen muchas soluciones algorítmicas propietarias que son especialmente útiles para solucionar los problemas de identificación de gran escala. Esas soluciones fueron específicamente desarrolladas para MegaMatcher, incorporando aspectos de los algoritmos VeriFinger, VeriLook, VeriSpeak y VeriEye. Algunas de esas soluciones se mencionan en las siguientes descripciones de los motores biométricos de identificación de huellas, rostros, voz e iris.

### *Motor de Extracción y comparación dactilar MegaMatcher*

- **Total compatibilidad MINEX.** NIST reconoció al algoritmo MegaMatcher como compatible con MINEX y apropiado para su uso en los programas de verificación de identidad personal (PIV).
- **Comparación de huellas planas y roladas.** El motor dactilar MegaMatcher compara huellas planas y roladas entre sí. Los algoritmos convencionales de identificación de huellas “planas” realizan la comparación entre huellas planas y roladas de manera poco confiable debido a las deformaciones específicas de las huellas roladas. MegaMatcher permite comparar huellas planas-planas, planas-roladas o roladas-roladas con un altísimo nivel de confiabilidad y precisión. El algoritmo compara hasta 200,000 registros de huellas planas por segundo en un PC.
- MegaMatcher puede **determinar la calidad de imagen dactilar**, que puede usarse durante la captura para garantizar que sólo las plantillas dactilares de mejor calidad lleguen a la base de datos.

- Se utiliza **generalización de plantillas** para crear plantillas de una mejor calidad a partir de varias imágenes del mismo dedo. Plantillas de mejor calidad proporcionan un nivel más alto de precisión al identificar.
- MegaMatcher es **tolerante a traslación, rotación y deformación de huellas**. Utiliza un algoritmo de comparación propietario que identifica las huellas incluso si están rotadas, repositionadas o deformadas.
- El algoritmo de **filtrado adaptivo de imágenes** elimina ruidos, rupturas y truncados, garantizando una extracción confiable de minucias incluso a partir de huellas de muy baja calidad en menos de 1 segundo.

### *Motor de extracción y comparación facial MegaMacher.*

- La **tolerancia a la posición del rostro** garantiza un nivel de captura conveniente. MegaMatcher permite 360 grados de giro. Inclinación lateral de hasta 15 grados en cada dirección desde la posición frontal. Rotación de hasta 45 grados en cada dirección desde la posición frontal. Vea las especificaciones técnicas para más detalles.
- **Detección confiable del rostro** garantiza una captura precisa desde cámaras, webcams y diversos documentos digitalizados; los rostros se pueden capturar desde páginas escaneadas de pasaportes u otros tipos de documentos. Cuando existen **múltiples rostros** en el video o imagen, se pueden capturar y procesar simultáneamente. Opcionalmente se puede detectar el **género** de la persona, puntos de características faciales y **emociones básicas**.
- **Reconocimiento de atributos faciales**. MegaMatcher puede configurarse para detectar ciertos atributos durante la extracción – **sonrisa, boca abierta, ojos cerrados, anteojos y gafas de sol**.
- **Detección de rostro vivo**. Un sistema convencional de identificación facial puede ser engañado colocando una fotografía frente a la cámara. MegaMatcher puede evitar este tipo de brecha de seguridad al determinar si el rostro presente en un video está “vivo”

o es una fotografía. Vea más adelante el detalle de las recomendaciones para la detección de rostro vivo.

- La plantilla del registro biométrico puede contener **varias muestras de la misma persona**. Esas muestras se pueden capturar de distintas fuentes y en distintos momentos, permitiendo así mejorar la calidad de la comparación. Por ejemplo una persona puede ser ingresada al sistema vistiendo anteojos y sin ellos, o con diferentes tipo de gafas; con y sin barba y bigote, etc.

### *Motor de extracción y comparación de iris MegaMatcher*

- **Confiabilidad probada por NIST IREX.** El motor de comparación de iris MegaMatcher está basado en VeriEye, reconocido por NIST como uno de los algoritmos más confiables y precisos de reconocimiento de iris disponibles en el mercado.
- **Comparación rápida.** La velocidad de comparación de iris es de hasta **200,000 comparaciones por segundo** en un PC. Vea la sección de “especificaciones técnicas” para más detalles.
- **Detección robusta.** Detecta iris aún con obstrucciones en la imagen, ruido visual y/o diferentes niveles de iluminación. Se eliminan obstrucciones por reflejos, párpados y pestañas. También acepta imágenes de ojos entrecerrados y miradas indirectas.
- **Detección automática de entrelazado y corrección** de imágenes de iris en movimiento para plantillas de máxima calidad.
- **Correcta segmentación del iris** incluso cuando no hay círculo perfecto, cuando el centro y borde del iris son diferentes, cuando el contorno no es ni círculo ni elipse o cuando el borde parece un círculo perfecto.

### *Mega Matcher y MegaMatcher Acelerator en Sistemas de Alta*

#### *Productividad*

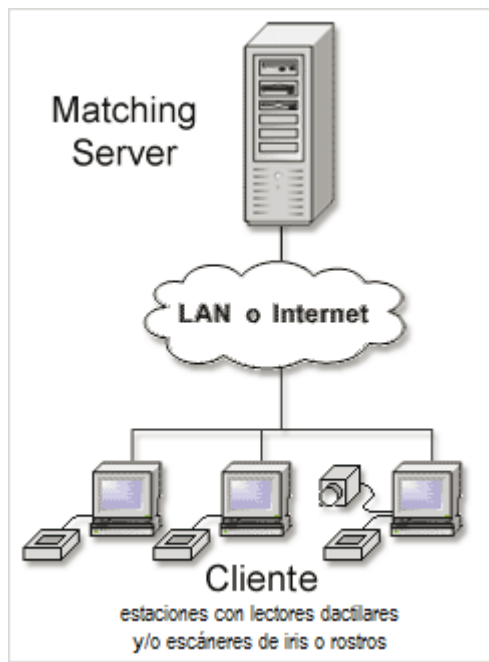
Diferentes proyectos biométricos de gran escala, tienen requerimientos específicos de desempeño. El grupo de motores y arquitecturas de comparación MegaMatcher puede usarse

de las siguientes formas dependiendo de la velocidad de comparación requerida, el tamaño de la BD y la disponibilidad del sistema:

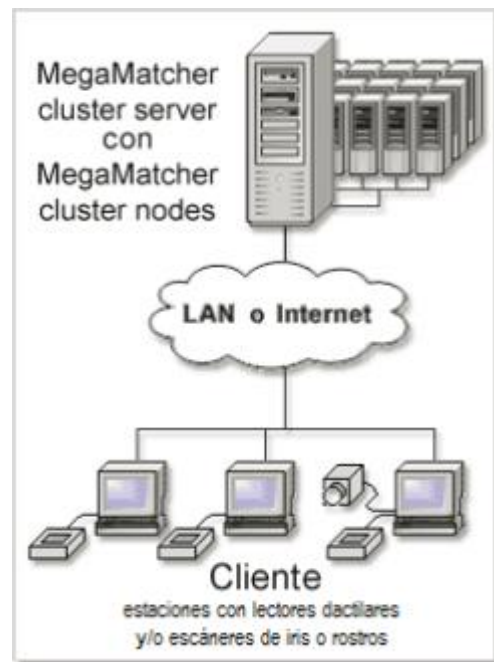
- Servidor de Comparación Unitario;
- Clúster de PC ejecutando componentes MegaMatcher;
- Una unidad MegaMatcher Accelerator 7.0 Standard o Extended (vea el catálogo “MM Accelerator”);
- Clúster de MegaMatcher Accelerator 7.0 Standard o Extended (vea el catálogo “MM Accelerator”).

Es posible usar más de una arquitectura dentro de un sistema biométrico de gran escala para conseguir un óptimo desempeño y/o disponibilidad del sistema. Por ejemplo, se pueden utilizar unidades MegaMatcher Accelerator 7.0 para selección de candidatos usando iris o varias huellas, y luego validar los resultados en el Servidor de Comparación o el Clúster con otras modalidades biométricas. Además, se pueden conectar dos o más Clústeres de Servidores o de MegaMatcher Accelerator 7.0 para lograr un sistema de alta disponibilidad.

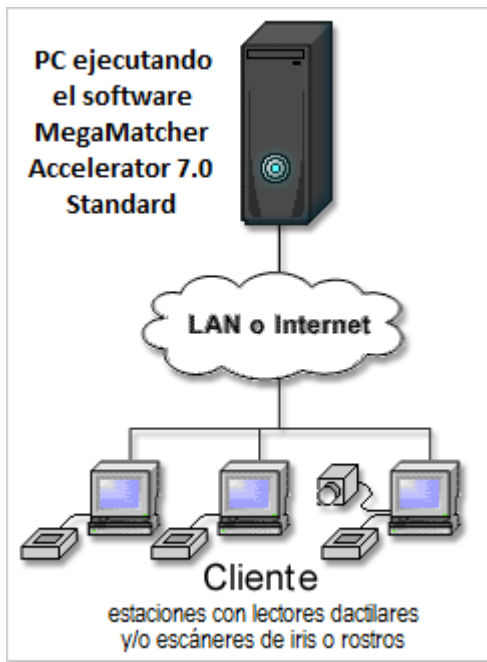
Estos gráficos comparan las arquitecturas MegaMatcher SDK para sistemas AFIS de alto desempeño:



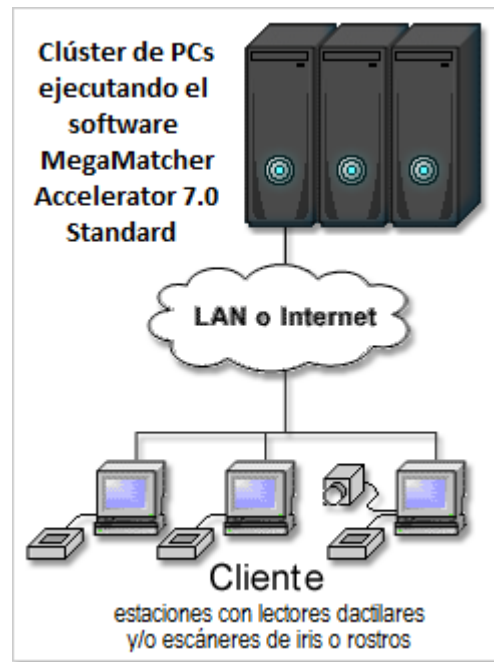
*Compara 200,000 huellas, rostros o iris por segundo. Requiere MegaMatcher 5.1 Standard SDK.*



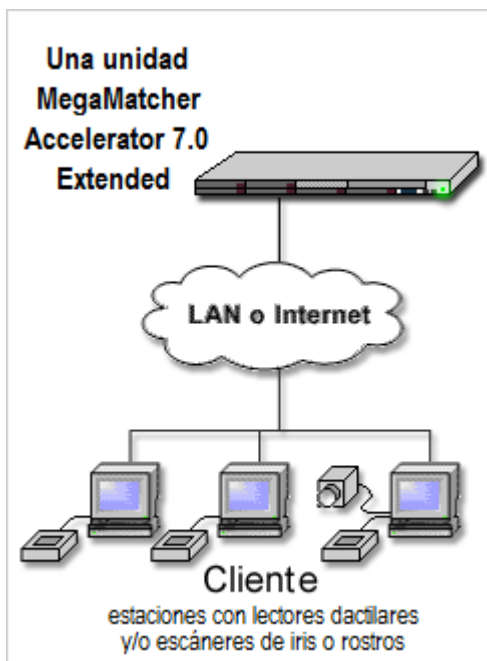
*Compara hasta varios millones de huellas, rostros o iris por segundo. Requiere MegaMatcher 5.1 Extended SDK.*



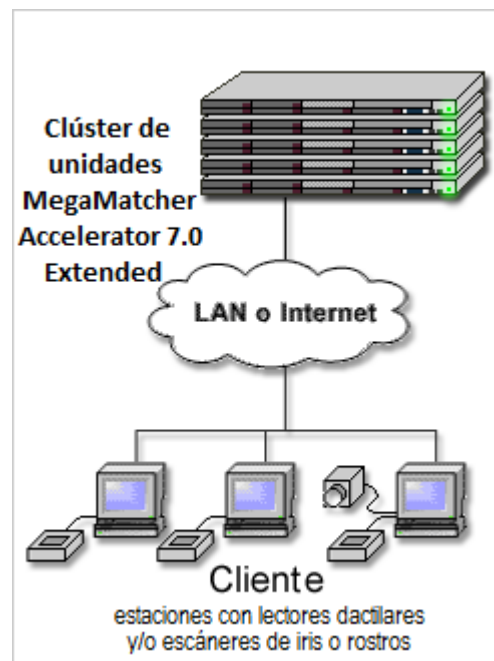
Compara 35,000,000 de huellas o 70,000,000 de iris o 35,000,000 de rostros por segundo. Requiere MegaMatcher 5.1 Extended SDK para el desarrollo de la aplicación cliente y 1 instalación del software MegaMatcher Accelerator 7.0 Standard.



Compara desde 70,000,000 a 350,000,000 de huellas o desde 140,000,000 a 700,000,000 de iris o desde 70,000,000 a 350,000,000 de rostros por segundo. Requiere MegaMatcher 5.1 Extended SDK para desarrollar la aplicación cliente y múltiples instalaciones del software MegaMatcher Accelerator 7.0 Standard para alcanzar el desempeño óptimo.



Compara 100,000,000 de huellas o 200,000,000 de iris o 100,000,000 de rostros por segundo. Requiere MegaMatcher 5.1 Extended SDK para desarrollar la aplicación cliente y 1 unidad MegaMatcher Accelerator 7.0 Extended.



Compara desde 200,000,000 hasta varios billones de huellas, o desde 400,000,000 hasta varios billones de iris, o desde 200,000,000 hasta varios billones de rostros por segundo. Requiere MegaMatcher 5.1 Extended SDK para desarrollar la aplicación cliente y múltiples unidades MegaMatcher Accelerator 7.0 Extended para alcanzar el desempeño óptimo.

### *Servidor de Comparación Unitario*

La arquitectura con un único Servidor de Comparación puede usarse en sistemas de tamaño moderado como un AFIS local o sistema multibiométrico que no tenga requerimientos estrictos sobre el desempeño o disponibilidad. El Software Servidor de Comparación está disponible en MegaMatcher 5.1 Standard y Extended SDK, así como en VeriFinger 7.1 Extended SDK, VeriLook 5.6 Extended SDK, VeriSpeak 2.2 Extended SDK and VeriEye 2.9 Extended SDK.

Un PC ejecutando el software Servidor de Comparación acepta solicitudes de identificación de los componentes cliente para huellas, rostros y/o iris y devuelve los resultados de la tarea. Se pueden comparar hasta 200,000 huellas, rostros o iris por segundo en un Servidor de Comparación Unitario (con procesador Intel Core i7-4771 @ 3.5 GHz). También puede usarse el Servidor de Comparación para sistemas multibiométricos que utilicen cualquier combinación de las modalidades biométricas disponibles: huellas, rostros, voz y/o iris. Vea la sección de “especificaciones técnicas” para más detalles sobre cada motor de comparación.

## **DESCRIPCIÓN DE LOS COMPONENTES DE SERVER Y CLÚSTER**

### *Clúster Server*

Permite escalar un sistema de identificación biométrica a múltiples PC (nodos de clúster) vinculados a través de una red LAN o Internet. El Clúster Server divide la base de datos de plantillas biométricas y la distribuye entre los nodos del clúster. Cada nodo del clúster realiza la comparación de plantillas en la parte que le corresponde de la base de datos utilizando:

- El componente Fast Fingerprint Matcher o Fingerprint Matcher para la comparación de plantillas de huellas dactilares;

- El componente Fast Face Matcher o Face Matcher para la comparación de plantillas faciales;
- El componente Fast Iris Matcher o Iris Matcher para la comparación de plantillas de Iris.
- El componente Voice Matcher para la comparación de plantillas vocales.

A mayor número de nodos, la comparación es más rápida, porque cada nodo opera en una parte más pequeña de la base de datos.

Un nodo del clúster puede almacenar plantillas en una base de datos o utilizar la memoria RAM para lograr un mejor desempeño.

El componente Clúster Server puede usarse en Microsoft Windows, Linux y Mac OS X. Revise los requerimientos del sistema para más información sobre el la configuración de hardware recomendada.

El Software para ejecutar los nodos del clúster también se incluye junto con el Clúster Server. El software del nodo del clúster puede ejecutarse en un número ilimitado de equipos conectados al Clúster Server.

**El Módulo de Comunicación del Cliente** que permite enviar tareas al Clúster Server, consultar el estado de la tarea, obtener resultados y eliminar tareas del servidor, se incluye con MegaMatcher 5.1 SDK, VeriFinger 7.1 SDK, VeriLook 5.6 SDK, VeriSpeak 2.2 SDK and VeriEye 2.9 SDK éste módulo oculta todas las comunicaciones de bajo nivel y proporciona un API de alto nivel para el desarrollador.

Los componentes y los módulos de soporte para bases de datos con los códigos fuente incluidos para el componente Clúster Server se muestran en la siguiente tabla. El integrador puede desarrollar módulos personalizados para trabajar con otras bases de datos y utilizados con los componentes Clúster Server.

Se incluye una licencia del componente Clúster Server con MegaMatcher 5.1 Extended SDK. Los clientes MegaMatcher 5.1 SDK pueden adquirir más licencias en cualquier momento.

Es un software listo para usar diseñado para construir sistemas web de tamaño moderado y otros sistemas basados en red como AFIS locales o sistemas de identificación



multibiométrica. El software Server se ejecuta en un PC servidor y permite realizar la comparación de plantillas biométricas en el servidor usando:

- El componente Fast Fingerprint Matcher o Fingerprint Matcher para la comparación de plantillas de huellas dactilares;
- El componente Fast Face Matcher o Face Matcher para la comparación de plantillas faciales;
- El componente Fast Iris Matcher o Iris Matcher para la comparación de plantillas de Iris.
- El componente Voice Matcher para la comparación de plantillas vocales.

Se puede habilitar la **comparación multibiométrica fusionada** ejecutando componentes para comparación de huellas, rostros, iris y voz en la misma máquina. **El Módulo de Comunicación del Cliente** que permite enviar tareas al Matching Server, consultar el estado de la tarea, obtener resultados y eliminar tareas del servidor, se incluye con MegaMatcher 5.1 SDK, VeriFinger 7.1 SDK, VeriLook 5.6 SDK, VeriSpeak 2.2 SDK y VeriEye 2.9 SDK éste módulo oculta todas las comunicaciones de bajo nivel y proporciona un API de alto nivel para el desarrollador.

Los componentes y los módulos de soporte para bases de datos con los códigos fuente incluidos para el componente Matching Server se muestran en la siguiente tabla. El integrador puede desarrollar módulos personalizados para trabajar con otras bases de datos y utilizados con los componentes Matching Server.

El componente Matching Server requiere una licencia especial que permite ejecutar el componente en todas las máquinas que ejecuten los componentes de comparación de huellas, rostros, iris o palma de la mano obtenidos por un integrador. El software Matching Server se incluye con MegaMatcher 5.1 Standard SDK y MegaMatcher 5.1 Extended SDK.

Además el componente Matching Server se incluye con VeriFinger 7.1 Extended SDK, VeriLook 5.6 Extended SDK, VeriSpeak 2.2 Extended SDK y VeriEye 2.9 Extended SDK (vea sus catálogos para más detalles).

## ANEXO E

### DESCRIPCIÓN DE COMPONENTES DE LA PALMA DE LA MANO

#### *Palm Print Matcher*

Realiza la comparación de plantillas de palmas de mano en los modos 1:1 (verificación) y 1:N (identificación).

Las secciones de “Especificaciones Técnicas” y “Pruebas de Confiabilidad y Desempeño” contienen información sobre las velocidades de comparación y la calidad del reconocimiento.

Se incluye una licencia del componente Palm Print Matcher con MegaMatcher 5.1 Standard SDK y 2 licencias con MegaMatcher 5.1 Extended SDK. Los clientes MegaMatcher 5.1 SDK pueden adquirir más licencias en cualquier momento.

#### *Palm Print Client*

Crea plantillas de palmas a partir de imágenes de la palma de la mano. Además permite integrar soporte para formatos estándar de imágenes y plantillas de la palma de mano además de otros formatos de imagen en sistema biométricos nuevos o existentes basados en MegaMatcher SDK. Están soportados los siguientes estándares biométricos:

- **ANSI/NIST-ITL 1-2000** (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)
- **ANSI/NIST-ITL 1-2007** (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)
- **ANSI/NIST-ITL 1a-2009** (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)

El componente Palm Print Client permite la conversión entre nuestras plantillas propietarias de palma de la mano y plantillas ANSI/NIST-ITL.

El componente Palm Print Client también incluye:

- **WSQ (Wavelet Scalar Quantization)** Módulo para soporte para este formato de imagen. Este formato comprime una imagen de la palma de la mano hasta 10-15 veces. El proceso de compresión WSQ tiene “pérdidas”, por lo que la imagen comprimida no es igual al original (se pierde información). Sin embargo, el algoritmo WSQ fue especialmente diseñado para minimizar la pérdida de información dactilar, así la imagen reconstruida será lo más parecida posible al original.
- **JPEG 2000** Módulo para soporte para este formato de imagen.

El componente Palm Print Client puede usarse desde aplicaciones C/C++ y C# en todas las plataformas compatibles.

Se proporcionan wrappers .NET de librerías Windows para programadores .NET. Revise la sección de “especificaciones técnicas” para ver la velocidad de extracción de plantillas y el tamaño de la plantilla de la palma de la mano.

Se incluye una licencia del componente Palm Print Client con MegaMatcher 5.1 Standard SDK y MegaMatcher 5.1 Extended SDK. Los clientes MegaMatcher 5.1 SDK pueden adquirir más licencias en cualquier momento.

## **SEGURIDAD SIEMPRE A MANO**

### ***PalmSecure ofrece identificación personal simple y fiable***

Las únicas formas confiables de autenticación personal se basan en las características biométricas, y las venas de la palma de la mano humana están especialmente bien adaptados para la autenticación biométrica. Patrones de venas de la palma son únicos para cada persona - incluso los gemelos tienen diferentes patrones. FUJITSU PalmSecure es la tecnología biométrica más precisa, versátil y conveniente de su tipo en el mercado:

- **Máxima seguridad:** Las venas se ocultan debajo de la piel, y la identificación es, literalmente, y falsificación a prueba "en vivo", ya que las funciones de proceso sólo cuando la hemoglobina está fluyendo por las venas de una persona.

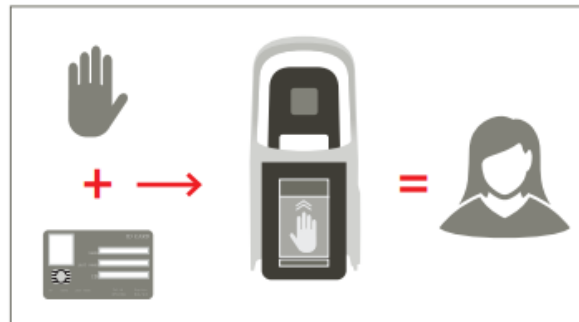
- Máxima precisión: Con una tasa de falsa aceptación de menos de 0,00008 por ciento, FUJITSU PalmSecure es el sistema de autenticación más preciso del mundo.
- Máximo rendimiento: El proceso de registro se completa en tan sólo diez segundos, y la identificación es completa en tan sólo uno o dos segundos - más rápido que cualquier solución contraseña.
- Altamente aceptada por los usuarios: La tecnología es sin contacto y por lo tanto completamente higiénico. La mano es simplemente aplaza el sensor - que hace PalmSecure fácil de usar.
- Muy versátil: La tecnología puede ser utilizada para el control de acceso al sitio, grabación de tiempo y las aplicaciones móviles, en la web y en el lugar de trabajo.
- Se utiliza en todo el mundo por los aeropuertos, bancos, empresas comerciales, centros de datos, los gobiernos, en el sector sanitario y en el sector minorista.

Y la tecnología PalmSecure tiene una ventaja adicional: Se puede combinar con otros métodos de autenticación. FUJITSU PalmSecure Identificación Partido ofrece un tipo de autenticación de dos factores que combina la tecnología PalmSecure único con tarjetas de identificación e insignias. La solución se basa en un dispositivo multifunción compacto. El dispositivo se compone de una pantalla táctil, la última placa del procesador ARM generación integrado, un lector multi-tarjeta y la tecnología PalmSecure alta seguridad de Fujitsu para la identificación personal y verificación basado en patrones de venas de palma. Fujitsu también ofrece un kit de desarrollo de software (SDK) con PalmSecure Identificación Partido para permitir una rápida integración en aplicaciones de Identidad de gestión de acceso realizadas por fabricantes de equipos originales e integradores.

### ***FUJITSU PalmSecure ID Match El apretón de manos digitales***

FUJITSU PalmSecure ID Match añade una nueva dimensión de la seguridad de insignias y tarjetas - sin importar si de acceso, datos o transacciones de pago deben ser salvaguardados. Esto se hace mediante la comparación de la palma de la mano de una persona con la identidad biométrica almacenada en el chip de una tarjeta inteligente. Este partido

Identificación asegura que el titular de la tarjeta es realmente el propietario legítimo. Esta solución de autenticación no requiere el almacenamiento de los datos biométricos personales en un servidor o en la nube. La comparación de la plantilla biométrica en la tarjeta - que está a sólo 1 KB a 2 KB de tamaño - con la palma del usuario se lleva a cabo directamente en la terminal de FUJITSU PalmSecure ID del partido (partido en el dispositivo).



FUJITSU PalmSecure ID Match supports very secure, ergonomic and convenient multi-factor authentication. The solution can also be used instead of passwords for all processes in critical infrastructures that require stringent identification control procedures.

FUJITSU PalmSecure ID Match evita el uso indebido derivado de robo de tarjeta o la divulgación de la PIN. Acceso no autorizado a los edificios o el uso de servicios se puede evitar, por no mencionar el robo y la manipulación de los datos y documentos personales oficial, o de negocios. La solución también es eficaz en la prevención del fraude en relación con la manipulación de los cajeros automáticos, transacciones bancarias electrónicas y tarjetas de identificación.

Fujitsu ofrece una plataforma completa solución compuesta de hardware, software y servicios para la optimización de las soluciones de seguridad existentes:

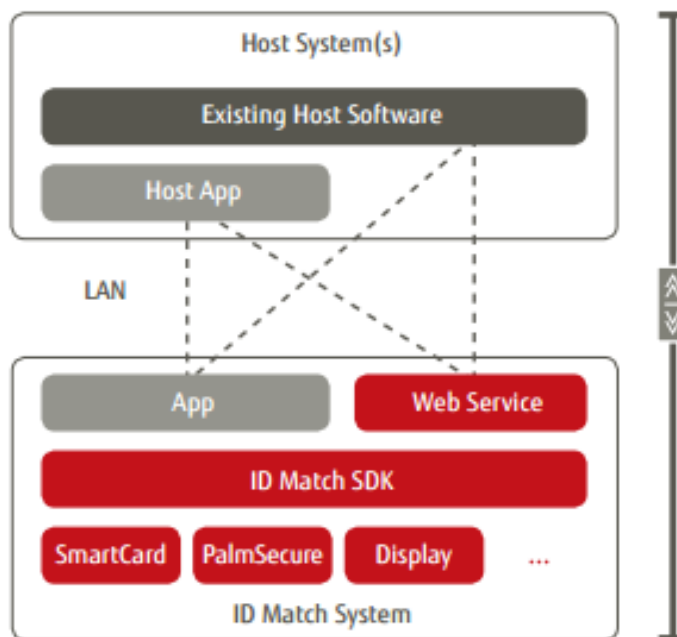
- El hardware, es decir, el terminal ID Partido, incluye la tecnología ARM altamente eficaz, características avanzadas de seguridad y todas las interfaces necesarias para aplicaciones de seguridad. La alta calidad, carcasa del dispositivo a prueba de manipulaciones con el sensor PalmSecure integrada permite intuitiva, la autenticación de dos factores touchfree, con una amplia flexibilidad de varios tipos de instalación o montaje.
- El software está basado en Linux. Un SDK permite a los socios y clientes para implementar la aplicación como parte de su solución de seguridad completa. Aplicaciones de demostración también se proporcionan como un medio de apoyo.
- Fujitsu apoya a los socios y clientes con programas de consultoría y formación en lo que respecta al desarrollo y la realización individual, soluciones de seguridad personalizada.

**FUNCIONES Y DESTACADOS**

**Plataforma segura para aplicaciones personalizadas**

FUJITSU PalmSecure ID Matches una plataforma compuesta de una pila de hardware y software, precisamente armonizado que proporciona un ambiente seguro para ejecutar la aplicación. La lógica de negocio está definida por la aplicación. Según el concepto del cliente, la lógica de la arquitectura de la solución se puede ejecutar en el terminal de ajuste de identidad o, ya sea parcial o totalmente, en el sistema host.

- Si el terminal ID de ajuste se utiliza como un sistema inteligente, mejora de la seguridad se entrega sin la necesidad de una base de datos y sin tener que almacenar datos biométricos personales de los usuarios.
- Si la lógica de negocio se ejecuta en un host, el terminal ID Partido sirve como el dispositivo de control, pero el proceso de partido no necesita necesariamente ser realizado por el propio terminal. Este concepto es útil cuando el escenario requiere que el usuario se autentica a sí mismo sólo una vez para obtener acceso a diversos servicios. El acoplamiento de un sistema de tiempo / asistencia, control de acceso físico, log-in PC, etc. es un ejemplo de esto en un ambiente de negocios.



The logic of the solution architecture can run on the ID Match terminal or, either partially or completely, on the host system.

### **La ID Match terminal: Conveniente. Eficaz. A prueba de vandalismo.**

Para los escenarios de autenticación de dos factores, FUJITSU ofrece PalmSecure Identificación Partido con el terminal ID Partido como un dispositivo muy eficiente equipado con un CPU ARM Cortex-A8 y un coprocesador criptográfico seguro, un montón de RAM y memoria flash rápido. El terminal elegante Identificación Partido cuenta con el uso intuitivo con una pantalla táctil de 4,3 pulgadas de cristal acrílico. La pantalla guía al usuario a través de todas las tareas de entrada. El juego de la palma de la mano con la identidad biométrica almacenada en la tarjeta inteligente se lleva a cabo sin problemas y en tan sólo segundos por el sensor extremadamente preciso FUJITSU PalmSecure integrado en el terminal.

El terminal ID Match es a prueba de vandalismo y resistente al desgaste gracias a los materiales de primera calidad, de los que se fabrica. El terminal puede ser utilizado como un dispositivo independiente o montado en la pared, e incluso se puede integrar en un sistema de POS. Los clientes que tienen carcasas de los aparatos hechos a medida también reciben ensamblajes que aseguran un ajuste perfecto. FUJITSU PalmSecure Identificación Partido soporta varios tipos de tarjetas. El módulo lector multi-tarjeta de la terminal de Identificación Partido cuenta con dos modos de toque libres y de contacto, así como la función de golpe. Externa y ranuras internas SAM, además de LAN y puertos USB, también se proporcionan. El dispositivo funciona con alimentación a través de Ethernet (PoE) o con alimentación externa a través de USB.

### **Arquitectura de software de alta capacidad**

La pila de software de FUJITSU PalmSecure Identificación Partido se basa en Linux y armonizado con el hardware de manera que todas las interfaces y dispositivos son compatibles a nivel de sistema operativo. La seguridad puede ser implementada a nivel lógico, por Ejemplo, en respuesta a las necesidades de los registros de sucesos constantes, una interfaz de administración segura o una función de auto-test. También se proporciona un mecanismo de recuperación de seguro, ya que es un mecanismo para la ejecución segura de código. El firmware del dispositivo se puede actualizar de forma segura con repositorios en paquetes;

esto también se aplica al firmware de los componentes internos tales como tarjetas y lectores de banda magnética.

Además, se proporciona un SDK para el acceso a las funciones del sistema y tareas administrativas. El SDK permite la integración solución flexible y minimiza el trabajo involucrado en el desarrollo de la aplicación final. Una aplicación de demostración está incluido en el SDK que muestra cómo la funcionalidad básica para el registro de datos en tarjetas inteligentes y funciona el proceso de adaptación. Esto proporciona a los desarrolladores un valioso apoyo al escribir programas que ofrecen una experiencia de usuario óptima. Otras características de soporte de desarrollo de aplicaciones incluyen una plantilla para escribir plug-ins específicos de la tarjeta, código de ejemplo y las implementaciones de contacto y sin contacto de tarjetas inteligentes.

### *Apoyo integral.*

Fujitsu lidera el camino hacia las identidades electrónicas seguras con PalmSecure - en el nivel físico, lógico y funcional - para asegurarse de que un usuario es de hecho la persona autorizada para obtener acceso a las tareas y funciones específicas. Los socios y los clientes reciben soporte completo para esta tecnología a través de servicios de consultoría y programas de capacitación. Al mismo tiempo, Fujitsu está haciendo importantes inversiones en la expansión del concepto PalmSecure y el desarrollo de soluciones, como la autenticación mutua basada en OpenLimit trueidentity® - este software permite la autenticación segura, así como la comunicación de datos segura a través de un canal seguro de datos. La gama de soluciones de socios disponibles para PalmSecure Identificación Partido, como la gestión de identidades que se integra fácilmente en cualquier infraestructura de TI, también se ampliará.



## ANEXO F

### TRADUCCIÓN DEL MANUAL SDK DEL REALPASS-F VERSIÓN 1.0

#### *FUNCIÓN BÁSICA*



### *Pantalla Principal:*

1. Seleccione pasaporte o cédula de identidad.
2. Seleccione la función de leer LECTURA NUMÉRICA, RFID, VIZ, el Código de Barras de los documentos
3. Seleccione la fuente de luz del dispositivo. ([LECTURA NUMÉRICA] - [infrarrojos], [VIZ] - [Blanco] están relacionados entre sí.)
4. Seleccione [Log] o [Resumen (ePassport)] función.

#### **Plantillas Puede guardar la configuración actual de las plantillas o carga**

- 1) RealPass Lista de plantillas: Seleccionar las plantillas básicas o plantillas definidas por el usuario.
- 2) Registrar/modificar/Borrar: Para el mantenimiento de las plantillas.

#### **[ePassport & eID Reader UI]**

- Estado del dispositivo
- Modelo y Número de serie
- Información SDK y Versión Demo

#### **[Images UI]**

- Infra-Red, White, and UV Images(RPF-U)

#### **[MRZ UI]**

- Machine Readable Zone Information and Checksum

#### **[RFID UI]**

- RFID Chip Información y seleccione la opción para la autenticación (AA,CA,PA,TA)

#### **[VIZ UI]**

- Operación Automatizada: En el caso del pasaporte (que ha registrado el pasaporte VIZ Plantilla depende de código de país). Para registrar pasaporte VIZ plantillas, consulte la sección 3.1 [Cómo registrar el nuevo VIZ plantilla.]
- Operación Manual:
  - Seleccione la plantilla de la lista de plantillas.

- Pulse [Get Viz(Manual)] botón y esperar.
- Después de la captura y reconocimiento, VIZ Información se muestran en la interfaz de usuario.



**[Log UI]**

- Sistema de Visualización and SDK log.

**[Summary UI]**

- Solamente ePassport (MRZ + RFID/Contact Verificación Curzada)
- Resumen de información de ePassport.
- Tiempo de proceso de OCR, RFID, VIZ.

**[Barcode UI]**

- Escanea la imagen completa y lee los códigos de barras de forma automática.
- Puede seleccionar tipo de código de barras y activar / desactivar dichos tipos.



### Contenidos del SDK

Directory	Sub Directory	Contents
SDK	Document	- RealPass SDK Reference Manual - RealPass-F_User_Manual - RealPassUX Demo Manual
	Driver	- RealPass Device Driver: RealPassDriver_x86_V1.01.exe(32bit OS) RealPassDriver_amd64_V1.01.exe(64bit OS)
	Include	- Header files: RealPass.h - Definition files: RealPassDef.h
	Bin	- SDK DLL files - Execution files: RealPassUXDemo.exe - Font directory : OCR B font files
	Example	- Examples showing the usage of the SDK. They are written in Visual C++, C#, Delphi, and VB.net

**Table 1 Directory Structure of the SDK**

## **USABILIDAD**

### **Compilación**

Para llamar a las API definidas en el SDK, RealPass.h debe ser incluida en los archivos de origen y directorios.

### **Usando la DLL**

Para ejecutar una aplicación compilada con el SDK, todos los archivos dll y el directorio de fuentes deben estar en el mismo directorio de la aplicación.

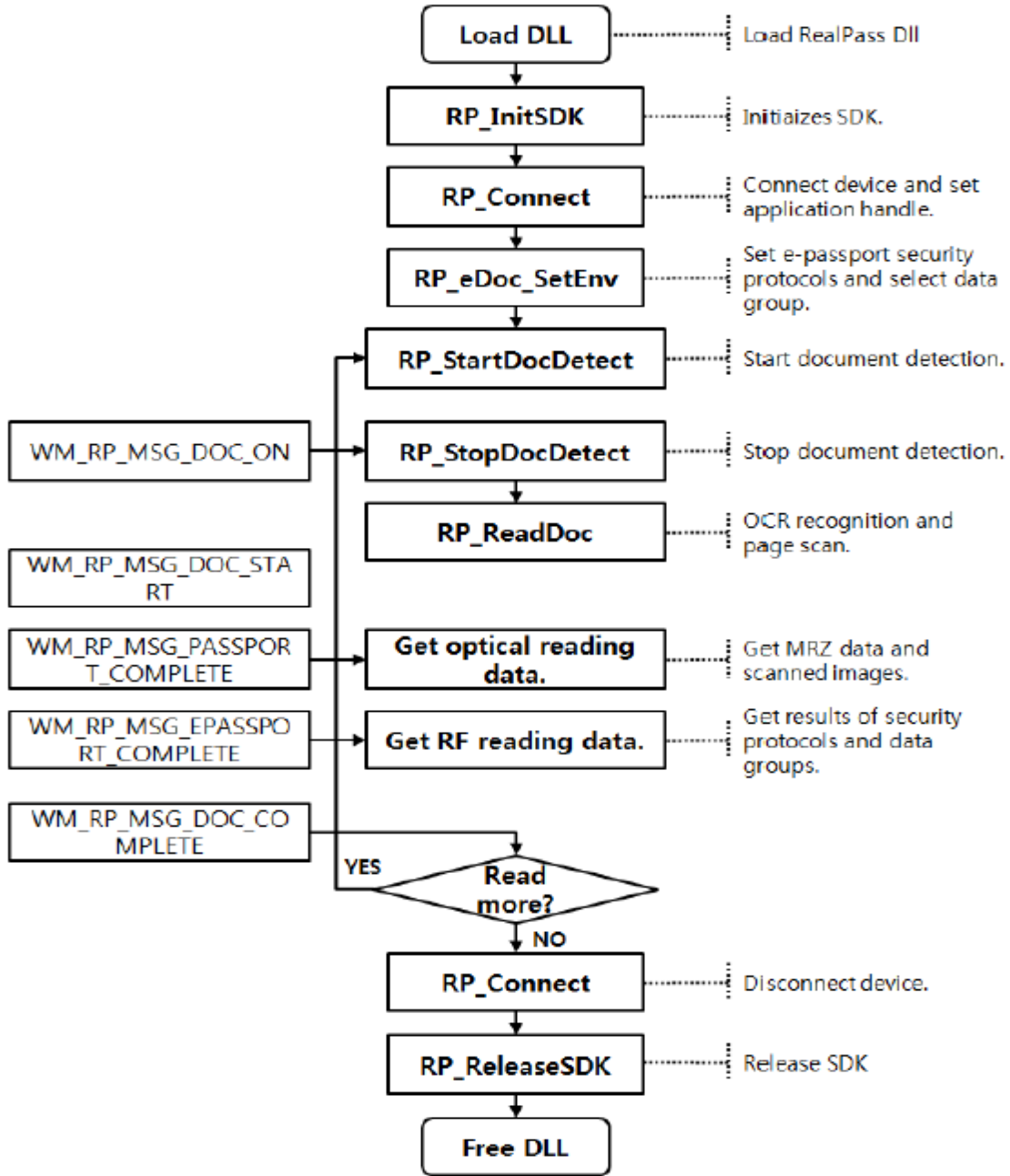
### **Tratamiento de mensajes de aplicaciones**

Para obtener un mensaje de RealPass, necesita contactar con los mensajes de ventana que vienen de la solicitud.

### **Guía de inicio rápido**

Este capítulo es para los desarrolladores que quieran empezar a trabajar rápidamente con RealPass SDK. Muestra cómo hacer las tareas más comunes con dispositivos RealPass para más ejemplos detallados, consulte el directorio de ejemplo del SDK.

**PROCEDIMIENTOS DE LECTURA DE DOCUMENTOS**



**Figura 1** Proceso de lectura de documentos

### *APIs de Ajuste de Ambiente*

- RP\_SetBatchScanMode: Modo de escaneo por lotes Conjunto.
- RP\_SetNewDocCheckMode: Modo de comprobación de set de documento.
- RP\_SetPreviewCallback: Establecer la función de devolución de llamada de pre visualización.
- RP\_SetBarcode: Código de barras Conjunto Enable/Disable.
- RP\_SetEnable: Modos de Juego Enable/Disable.
- RP\_GetEnable: Obtén modos Enable/Disable.
- RP\_SetBarcodeType: Establecer los tipos de códigos de barras.
- RP\_GetBarcodeType: Obtén tipos de códigos de barras.

### *La recolección de datos APIs*

- RP\_GetDocType: Comprueba el tipo de documento.
- RP\_GetMRZText: Obtén 88 caracteres de MRZ.
- RP\_GetMRZTextEx: Obtener los caracteres de las 3 líneas MRZ.
- RP\_ConvertMRZ: Convertir 88 caracteres en la estructura MRZ.
- RP\_ConvertMRZEx: Convertir 3 Línea MRZ en estructura de información MRZ.
- RP\_GetImage: Obtener imágenes escaneadas.
- RP\_SaveImage: Guarde las imágenes escaneadas a archivos.
- RP\_GetBarcodeCnt: Obtener cuenta de código de barras.
- RP\_GetBarcodeData: Obtener datos de código de barras.
- P\_GetVIZResult: Obtener datos de VIZ.

### *APIs del lector de e-Passport*

- RP\_eDoc\_SetEnv: Setear e-passport protocolos de seguridad y los grupos de datos seleccionados.
- RP\_eDoc\_SetFileName: Setear e-passport Registro y nombre del archivo de certificado.
- RP\_eDoc\_GetFileName: Obtener e-passport Registro y nombre del archivo de certificado.
- RP\_eDoc\_GetResult: Obtener resultados de los protocolos de seguridad y los grupos de lectura de datos.
- RP\_eDoc\_GetMRZ: Obtener 88 caracteres del DG1.