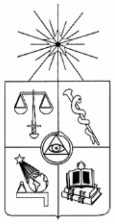

UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

VALIDACION BIOMETRICA EN EL PAGO DE BENEFICIOS DEL INSTITUTO DE PREVISION SOCIAL (IPS)

MEMORIA PARA OPTAR AL TITULO DE INGENIERO CIVIL EN COMPUTACION

Victor Hugo Maldonado Soto

PROFESOR GUIA :
Nancy Hitschfeld Kahler

MIEMBROS DE LA COMISION :
Benjamin Bustos Cardenas
Pablo Gonzalez Jure

SANTIAGO DE CHILE
ABRIL 2011

Resumen

El proyecto de validación biométrica tiene como objetivo principal el de diseñar e implementar una plataforma computacional que permita aplicar seguridad biométrica dactilar en el pago de beneficios del Instituto de Previsión Social (IPS).

Gracias a convenios suscritos entre el IPS y Bancoestado, el IPS puede utilizar toda la red de sucursales, oficinas y cajas vecinas, desplegadas en todo Chile, para el pago de beneficios a sus pensionados. Estos pagos se pueden hacer directamente al beneficiario o a su apoderado. El volumen de pagos que actualmente hace el IPS es de alrededor de 2.000.000 al mes por lo tanto la validación biométrica es una herramienta que permite asegurar el correcto destino de los millonarios pagos que hace el Estado de Chile a sus beneficiados.

El proyecto se basa en la posibilidad de comparar la huella dactilar física de una persona con la información de la huella que es provista en su cédula de identidad. La solución propuesta se compone de una parte cliente, encargada de capturar la información de huellas dactilares (desde el dedo y desde la cédula) y otra parte servidora, encargada del proceso de comparación de dichas huellas en la modalidad de matching 1 a 1.

La componente servidora del proyecto, encargada de efectuar el matching entre huellas, fue implementada por la compañía NEC. La componente cliente del proyecto se implementó en dos plataformas o canales de comunicación diferentes : canal caja finesse (cajas tradicionales instaladas en las sucursales del banco y en las oficinas serviestado) y canal caja vecina (cajas auxiliares instaladas en almacenes y negocios de barrio). Estas últimas poseen un subconjunto de las funciones de las cajas tradicionales.

La metodología utilizada fue la propuesta por el banco la cual es una adaptación de la metodología del ciclo de vida.

En esta memoria se diseñó parte de la arquitectura de la plataforma y se trabajó en el análisis y diseño de los módulos utilizados como interfaces en las cajas finesse. Estos módulos se implementaron en plataforma Windows XP SP1. La implementación del canal caja vecina fue hecha por la compañía Telefónica previa especificación de requerimientos y análisis funcional los cuales también son incluídos como parte del desarrollo de esta memoria.

La plataforma se validó a través de un criterio de aceptación basado en un protocolo de pruebas. Se instaló y probó satisfactoriamente una plataforma piloto en una sucursal tradicional y en una caja vecina.

Indice

1.- **Introducción** :

En la popular enciclopedia electrónica Wikipedia se define como **biometría** al estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. Mas específicamente define la "biometría informática" como la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo para "verificar" identidades o para "identificar" individuos.

Desde muy temprana edad sabemos que la huella dactilar es un rasgo propio de una persona y que no se repite entre un individuo y otro. Para obtener nuestra primera cédula de identidad hemos tenido que untar todos nuestros dedos con una tinta y luego plasmar nuestras huellas en una cartulina.

En la **Figura 1** se describen 7 puntos característicos que hay en un dedo, estos puntos son también llamados minutae o **minucias**.

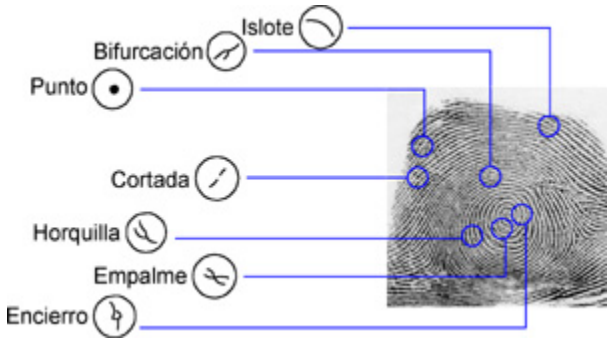

Figura 1 : Diferentes minucias presentes en una huella

Actualmente existen varios dispositivos y programas capaces de capturar y clasificar el contenido de una huella dactilar. A partir del conjunto de minucias, el software biométrico genera un modelo en dos dimensiones. Para ello, la ubicación de cada minucia se representa mediante una combinación de números (x,y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible.

			
El dedo es leído por un capturador de huellas	El dedo es codificado por el capturador	Una plantilla es generada y la imagen es comprimida	El capturador guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla

Figura 2 : Secuencia de generación de un prisma dactilar

Desde hace más de 100 años que la biometría dactilar se usa en labores criminalísticas. La invención del computador agregó el componente que faltaba para desarrollar la técnica biométrica y convertirla en una sofisticada tecnología que en la actualidad da cuenta de aplicaciones basadas en biometría ocular, biometría facial y otras.

A partir del año 2000, el Servicio de Registro Civil e identificación comenzó a incluir valiosa información en la cédula nacional de identidad. Aparte de los datos 'legibles' que tiene la cédula, en el reverso, en la parte superior izquierda se encuentra un código de barras bidimensional llamado bloque PDF-417 el cual almacena la siguiente información :

```
RUN                          9
Application Number          10
Apellido Paterno            30
Código de País               3
Fecha de Vencimiento         6
Número de Serie             10
Registro de Discapacidad     1
Tipo de Documento            1
Dedo Codificado              4
Tamaño del Archivo PC1       4
Archivo PC1                342
---------------------------
Largo del registro :       420
```

En el campo `Archivo PC1` vienen codificadas las minucias correspondientes a la impresión dactilar plana que pueden ser usadas para la verificación AFIS (Automated Fingerprint Identification System ó Identificación Automática de Impresiones Dactilares).

Figura 3 : Código de barras bidimensional disponible en las cédulas de identidad emitidas en Chile

El bloque PDF-417 es legible vía lector de código de barras. El estándar para la identificación automática de impresiones dactilares que utiliza el Registro Civil es el llamado AFIS-NEC.

Tenemos entonces por un lado la posibilidad de capturar el prisma de identificación de una persona directamente desde su huella dactilar y por otro la de leer el prisma que aparece informado en su cédula de identidad, con esto podremos saber si la persona que tenemos enfrente es o no la legítima dueña de esa identidad.

1.1.- **Contexto** :

Bancoestado mantiene convenios de pago y recaudaciones con una serie de instituciones del Estado y empresas privadas. El proyecto de biometría viene a complementar un macro proyecto para que se licitara el IPS donde se pretende habilitar seguridad biométrica en el pago de las pensiones que el IPS hace a sus beneficiarios

Los pagos del IPS se efectúan en dos de los canales o plataformas de que dispone el banco, que son muy diferentes entre sí pero que conceptualmente corresponden a la parte cliente de la plataforma que se pretende implementar :

i.- Caja convencional (finesse) : Son las habilitadas en todas las sucursales tradicionales del banco, también se ocupan en las oficinas serviestado.

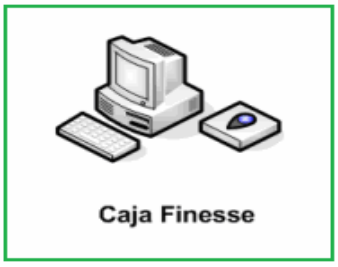

Figura 4 : Caja tradicional o finesse, presente en todas las sucursales del banco

El canal finesse opera en plataforma windows, esto permite tener gran flexibilidad al momento de implementar soluciones ya que este sistema operativo es compatible con múltiples aplicaciones y tiene la posibilidad de interactuar con servicios web.

La red de sucursales está distribuída a lo largo de todo Chile y constituye una de las redes de oficinas bancarias de mayor cobertura nacional.

ii.- Caja Vecina (Point of sales, POS) : Son cajas auxiliares instaladas en almacenes y negocios de barrio, poseen un subconjunto de las funciones de las cajas finesse.

Figura 5 : Caja vecina, presente en gran cantidad de almacenes y locales de barrio

Tanto el hardware como el software que lo componen son propietarios, operan a través de socket TCP/IP, por lo tanto requieren de un desarrollo especial.

La componente servidora de la plataforma fue implementada por la empresa NEC. Se incluyó en el contrato la entrega de un SDK (Software Development Kit) para web services de integración, la implementación de un log biométrico que almacene la información de las transacciones y una consola de administración del servidor biométrico.

1.2.- **Objetivos** :

El proyecto de validación biométrica tiene como objetivo principal el de diseñar e implementar una plataforma computacional que permita aplicar seguridad biométrica dactilar en el pago de beneficios del Instituto de Previsión Social.

Como objetivos secundarios se pueden mencionar los siguientes :

- Diseño de arquitectura de la plataforma que permita contextualizar y dar soporte a la construcción de dicha plataforma.

- Diseño de interfaces para caja finesse que permita la interacción con los dispositivos de captura y la comunicación con el servidor biométrico.

- Disminución en el tiempo de atención de los beneficiarios en caja.

- Creación de las bases para un servicio central de biometría multicanal y multisistema que permita efectuar soporte y asesoría en el tema de autenticación de personas.

1.3.- **Descripción de los requerimientos** :

1.3.1.- **Requerimiento principal** :

- *Implementar validación biométrica en el pago de beneficios del IPS.*

Esta implementación debe instalarse en los canales de caja finesse y caja vecina. La validación se efectúa sobre el beneficiario o sobre el apoderado que esté definido en el sistema de convenios.

La implementación debe tener la flexibilidad de omitir la validación cuando ésta no pueda efectuarse.

- *El nuevo modelo de operación del proceso de pago debe constar de tres etapas :*

i) Validación biométrica del beneficiario.

ii) Consulta de disponibilidad del beneficio IPS (actualmente se efectúa sin validación).

iii) Pago de beneficio IPS (actualmente se efectúa sin validación).

Para poder efectuar el pago de un beneficio del IPS, las etapas i) y ii) deben ser ejecutadas satisfactoriamente, no será posible llegar a la etapa iii) sin que las previas hayan sido ejecutadas.

1.3.2.- **Requerimientos secundarios** :

Requerimientos complementarios son los siguientes :

i) *Mantener un registro biométrico que permita obtener estadísticas de las transacciones de calce, independiente de su resultado*

ii) *Efectuar 'tunning' al proceso de calce de tal manera de evitar falsas aceptaciones y falsos rechazos.*

iii) *Sentar las bases para la instalación de un servicio central de biometría.*

1.4.- **Definiciones iniciales** :

Este apartado está orientado a entregar la referencia de conceptos y procesos que son nombrados en el presente documento.

Canal : Servicio de comunicación entre un punto de atención a público y los servicios centrales del banco.

DMA : Dynamic matching array, software biométrico centralizado.

Servidor de match : Servidor de comparación biométrico.

API : Rutina de interfaz de programación

Log biométrico : Registro de las transacciones efectuadas en un proceso de validación biométrico. Tiene por objeto hacer una consulta posterior por necesidad de los canales o de auditoria.

Job controller : Aplicativo que maneja la comunicación con los servidores de match, conversión de los formatos Afis y administración de la grabación al sistema de log biométrico.

Bloque Pdf 417 : Bloque que almacena información en código de barras bidimensional, contiene información de la minucias del dueño de la cédula de identidad en formato Afis-NEC.

Afis 378 : Código estándar para representar las minucias de las huellas dactilares.

Listener tcp : Interfaz diseñada para integrar los web service que expone la solución de NEC a un protocolo estándar de comunicación tcp, para uso en canal caja vecina.

Matching 1 a 1 : Proceso de validación biométrico que se basa en la comparación de dos argumentos que son, el código que representa la información de la cedula de identidad (pdf 417) y el registro de la huella digital (Afis 378).

Nota : Este proceso dentro de la solución provista por NEC tiene una duración que se encuentra en el rango de los 15 a 20 milisegundos.

Conversión Afis 378 – Afis-NEC : Proceso que se requiere para la interacción entre los lectores de huella y el estándar utilizado por NEC para la comparación 1 a 1, este proceso estará delegado al job controller y requiere ser programado.

Definición de txn : Una transacción biométrica es operación de comparación entre huellas y su correspondiente resultado, incluye como mínimo los siguientes elementos : header banco, información del Pdf 417, información del código Afis 378, Afis NEC, crc (número único identificador de una transacción) y el score (puntaje) de la operación.

1.5.- **Contenido de la memoria** :

El énfasis de lo realizado en esta memoria está en el análisis y diseño de interfaces para la plataforma de caja finesse ya que la solución de caja vecina (POS) fue implementada por la empresa Telefónica.

En el capítulo dos se describe la metodología utilizada en el desarrollo.

El análisis funcional, análisis de casos de uso y los criterios de validación de la plataforma son abordados en el capítulo tres.

Dada la importancia que adquiere la Arquitectura del sistema, ésta es abordada en el capítulo cuatro dejando para el capítulo cinco la descripción del diseño de las piezas de software que fue necesario construir para el funcionamiento de la plataforma.

En el capítulo seis se describen las pruebas efectuadas y finalmente en el capítulo siete son descritas las conclusiones del presente trabajo.

Mi participación en el proyecto se resume en lo siguiente :

- Análisis de requerimientos y análisis funcional de caja vecina y caja finesse

- Arquitectura de la plataforma.

- Análisis y diseño de interfaces para el canal caja finesse.

- Pruebas de conectividad y desempeño de lectores de huella y cédula de identidad.

La componente servidora del proyecto, encargada de efectuar el matching entre huellas, fue encomendada a la compañía NEC.

2.- **Metodología** :

La metodología utilizada es una adaptación de la metodología del ciclo de vida.

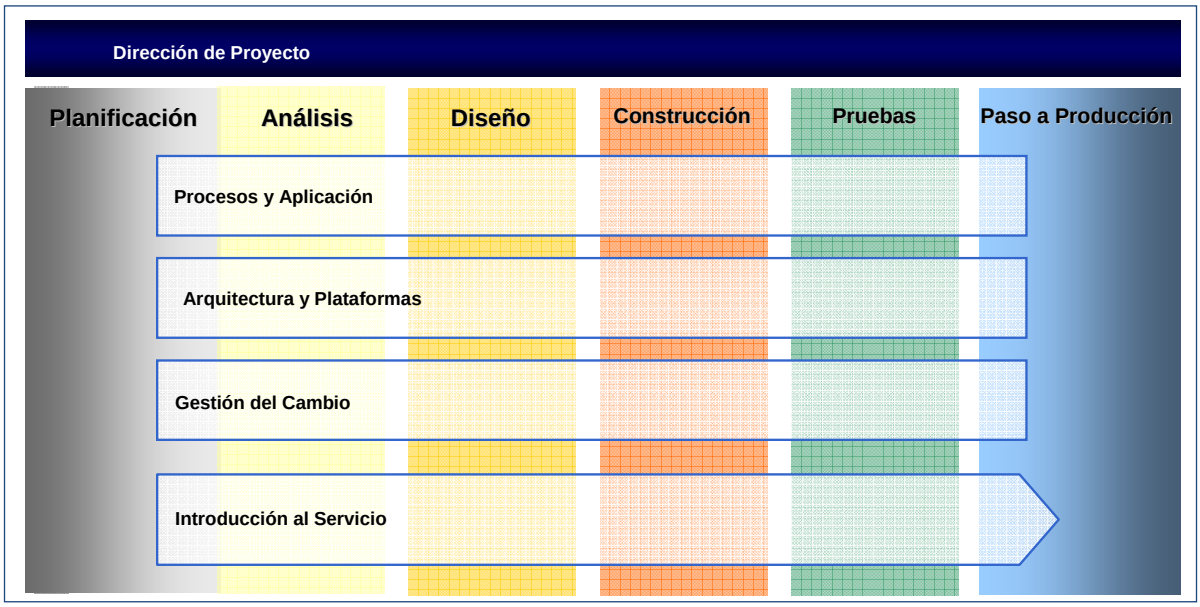

Figura 6 : Etapas y frentes de la metodología

Se distinguen 6 etapas del ciclo de vida y 4 frentes transversales a dicho ciclo, esta metodología es la actualmente usada en el desarrollo de proyectos del banco.

La etapa de planificación es similar en todos los frentes, las tareas involucradas son especificadas en la **Figura 7** :

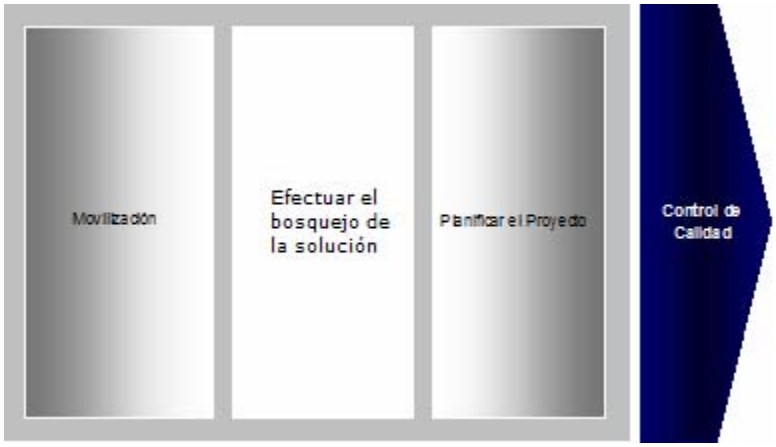

Figura 7 : Etapa de planificación

La tarea de movilización consiste en las primeros aprontes para abordar el desarrollo del proyecto, se efectúan reuniones de análisis, se definen las áreas responsables y cuál será la interacción entre ellas.

Una vez distribuidas las responsabilidades del nuevo desarrollo se comienza a efectuar el bosquejo de la solución, esto es una aproximación o consideración de los caminos viables para resolver cada uno de los frentes del proyecto.

Finalmente, cada uno de los frentes que compongan un determinado proyecto debe ser planificado, la herramienta de planificación que se utiliza es la muy conocida carta gantt.

Respecto de las frentes y etapas, especificaremos sólo el detalle de los 2 frentes más relevantes en el desarrollo de este proyecto que son frente de procesos y aplicación y frente de arquitectura y plataformas.

La nueva metodología propuesta por el banco define una actividad transversal a todos los frentes y etapas, se trata del control de calidad para la cual se ha creado un equipo de trabajo especial encargado de monitorear el porcentaje de adherencia a la nueva metodología.

2.1.- **Frente de Procesos y Aplicación** :

2.1.1.- **Etapa de Análisis** :

En esta etapa comienza con la identificación y análisis de los requerimientos que el desarrollo debe satisfacer, como parte del análisis se definen los casos de uso que deben ser considerados.

También en esta etapa se definen los procesos necesarios para llevar a cabo el proyecto sean estos procesos en línea, batch o una combinación de ambos.

Se incluyen en esta etapa definiciones de interfaz de usuario, piezas de software y definición de modelo de datos, también se deben determinar las necesidades de conversión y/o migración de datos.

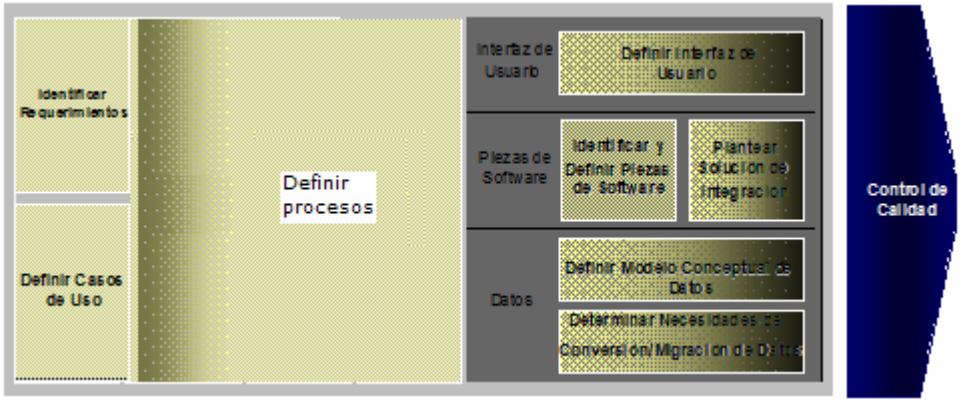

Figura 8 : Frente de procesos y aplicación, etapa de análisis

2.1.2.- **Etapa de diseño** :

En esta etapa se hacen los diseños de interfaz de usuario, también los diseños de las piezas de software que serán parte del desarrollo y la integración o ensamble de todas las piezas que compondrán el desarrollo.

También acá se diseña el modelo lógico de datos y la conversión y/o migración de datos, las particularidades de este proyecto hace que no exista la necesidad de elaborar un modelo lógico de datos ni tampoco efectuar migración de datos.

La tarea de diseño de plan de pruebas recae en el rol de usuarios operativos del sistema, en nuestro caso son los encargados operativos de los sistemas de caja vecina y caja tradicional.

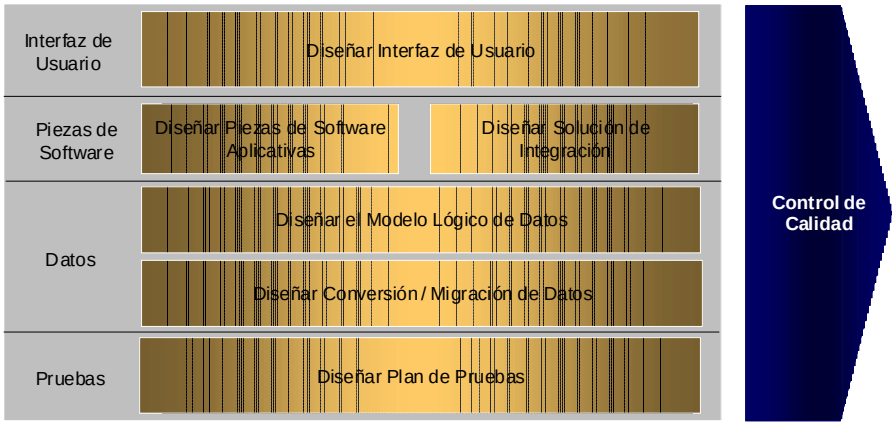

Figura 9 : Frente de procesos y aplicación, etapa de diseño

2.1.3.- **Etapa de construcción** :

En la mayoría de los desarrollos esta etapa es la mas extensa en duración. Este proyecto de memoria se basa en software biométrico ya construido, no obstante eso, se construyeron interfaces de usuario, interfaces de comunicación en las componentes cliente e interfaces para servidores web. Se hicieron pruebas unitarias de los componentes construidos y pruebas de integración entre componentes.

Las tareas a efectuar en la etapa de construcción se muestran en la **Figura 10** presente en la siguiente página.

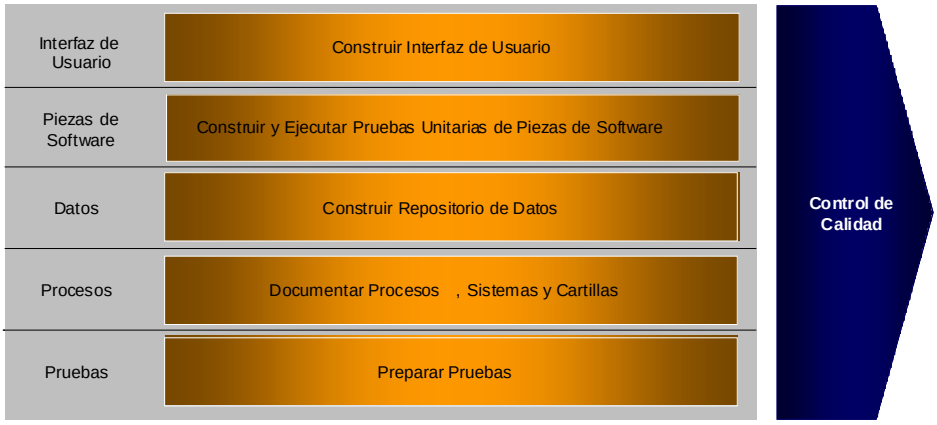

Figura 10 : Frente de procesos y aplicación, etapa de construcción

2.1.4.- **Etapa de pruebas** :

Esta etapa es fundamental en la metodología del ciclo de vida. En este proyecto se efectuaron exhaustivas pruebas a los dispositivos de lectura de huellas y de cédulas de identidad, también pruebas de performance sobre los dispositivos. Pruebas de conversión de datos, de procesos y de ensamble recién pudieron ser efectuadas con el montaje de la plataforma. Las pruebas de aceptación de usuarios fueron hechas a partir de la habilitación de la plataforma en una sucursal piloto del banco.

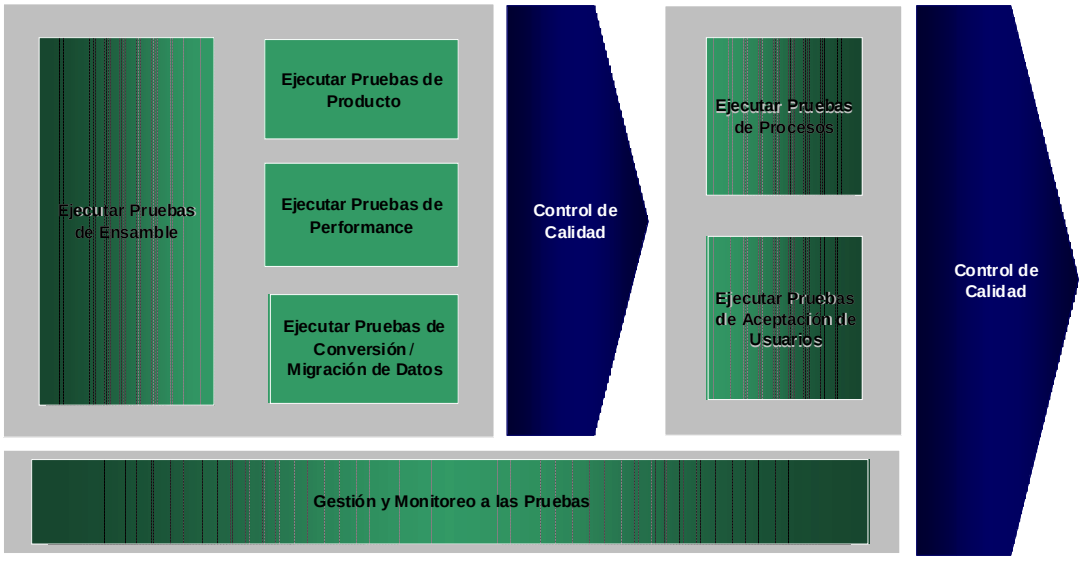

Figura 11 : Frente de procesos y aplicación, etapa de pruebas

2.1.5.- **Etapa de paso a producción** :

Esta es la última etapa del frente de procesos y aplicación, al cierre de este trabajo, la plataforma computacional aún no era puesta en producción, las tareas que sugiere la metodología son las siguientes :

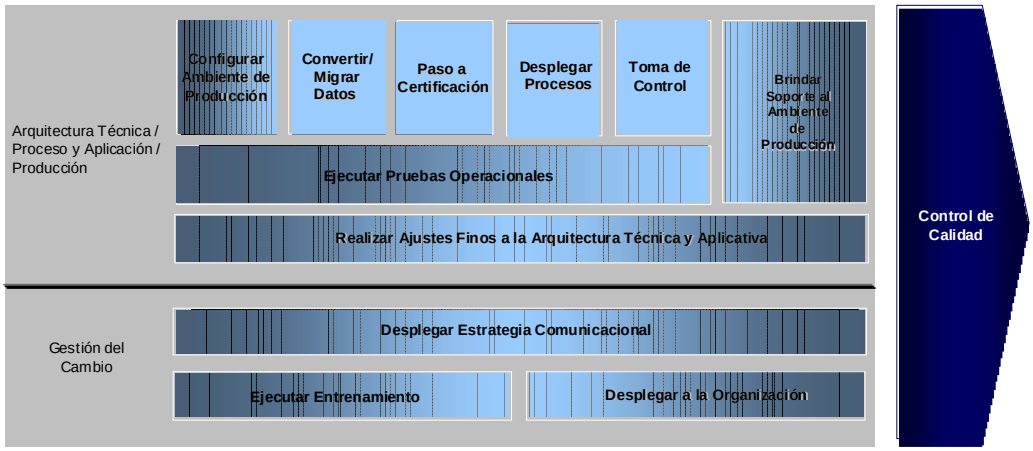

Figura 12 : Frente de procesos y aplicación, etapa de paso a producción

2.2.- **Frente de Arquitectura y plataformas** :

Este frente es muy importante en el desarrollo de este proyecto de memoria por cuánto trata de la implementación de una plataforma computacional para efectuar validación biométrica.

2.2.1.- **Etapa de Análisis** :

A partir de los requerimientos técnicos se define la arquitectura de la aplicación y esta a su vez permite definir la infraestructura del proyecto.

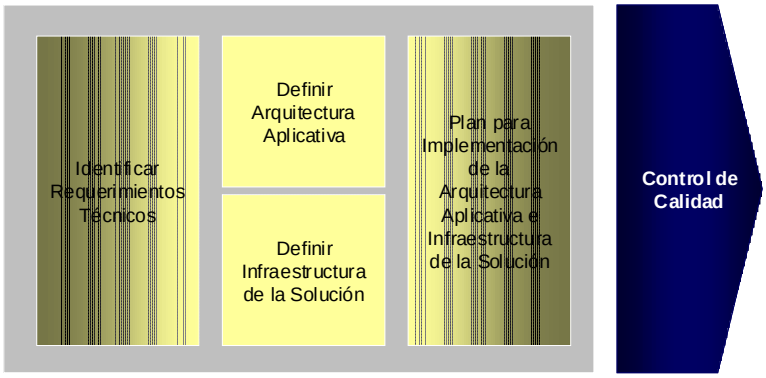

Figura 13 : Frente de arquitectura y plataformas, etapa de análisis

2.2.2.- **Etapa de diseño** :

Para la arquitectura de la plataforma se identifican y diseñan los componentes comunes, también se especifica la interacción entre ellos. Se diseña la infraestructura necesaria para los diferentes ambientes y finalmente un plan de pruebas que permita validar la arquitectura diseñada.

Figura 14 : Frente de arquitectura y plataformas, etapa de diseño

2.2.3.- **Etapa de construcción** :

Esta etapa tiene dos sub-etapas, por un lado lo referido a la arquitectura aplicativa y por otro la instalación y prueba de los ambientes de desarrollo, pruebas y producción.

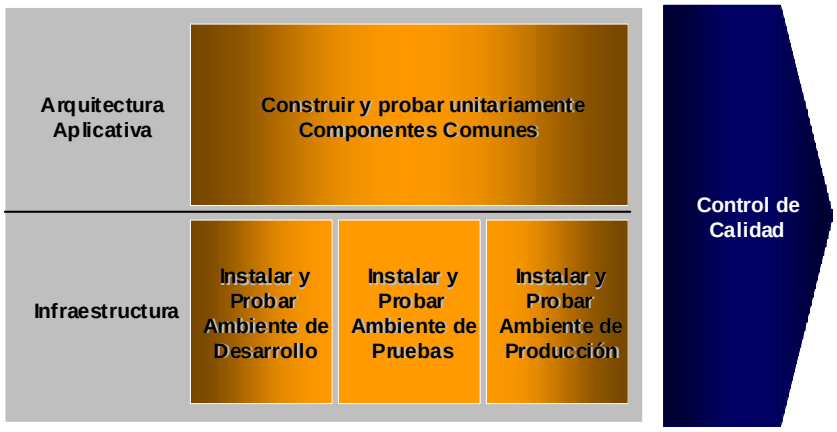

Figura 15 : Frente de arquitectura y plataformas, etapa de construcción

2.2.4.- **Etapa de pruebas** :

Se efectúan pruebas en los distintos ambientes, las pruebas en desarrollo fueron básicamente pruebas a los dispositivos lectores y al software biométrico en forma 'unitaria'. En ambiente de test existe un laboratorio en que se prueban los cambios en los canales de cajas, la pruebas en ambiente de producción se hicieron vía una plataforma piloto instalada en una sucursal.

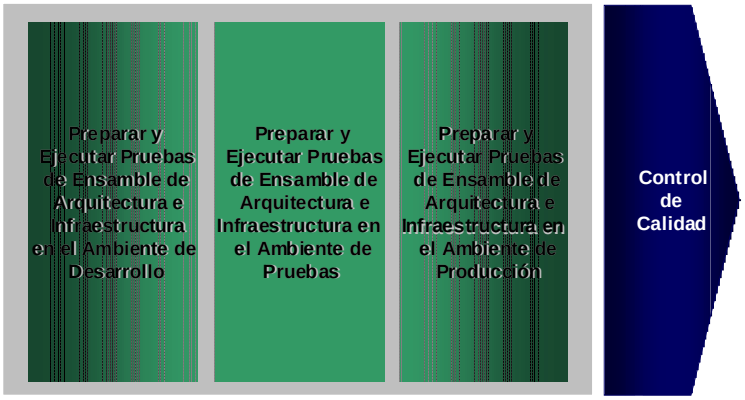

Figura 16 : Frente de arquitectura y plataformas, etapa de pruebas

3.- **Análisis** :

El proyecto se concibe y se hace viable a partir de la tecnología de calce de imágenes disponible en el mercado nacional. La gerencia del área de sistemas evaluó dos propuestas de solución para la componente servidora de la plataforma siendo finalmente seleccionada la propuesta de la compañía NEC. Esta solución provee un esquema de servidores especializados que permiten realizar los procesos de comparación en la modalidad de match tipo 1 a 1.

La técnica de reconocimiento se basa en el análisis de los puntos de minucias, específicamente en la ubicación y dirección de cada punto.

El software responde a una relación entre errores versus sensitividad en la lectura de las huellas. Mientras más sensible es el lector disminuye la tasa de falsa aceptación y aumenta la tasa de falso rechazo. A la inversa, con un dispositivo menos sensible, aumenta la tasa de falsas aceptaciones y disminuye la tasa de falsos rechazos, gráficamente la situación es la siguiente :

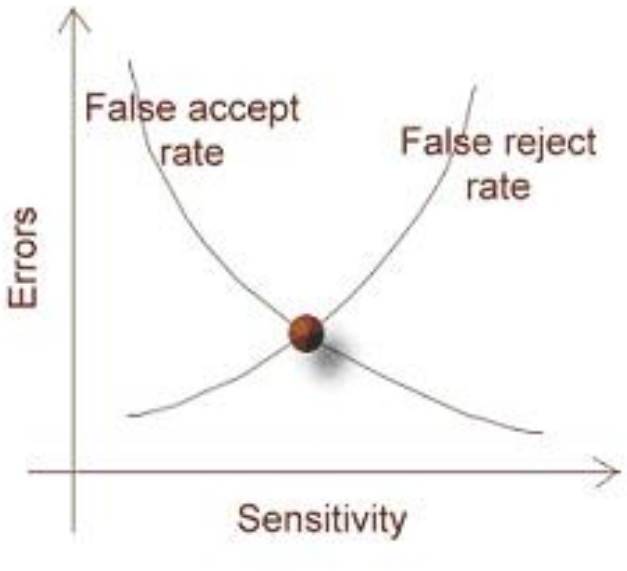

Figura 17 : Patrón de comportamiento de un software de comparación biométrica

El análisis se orienta a la implementación de una plataforma computacional que permita aplicar validación biométrica en dos de los canales de que dispone el banco para su oferta de servicios. Estos canales son, caja finesse, que corresponde a las cajas tradicionales instaladas en las sucursales y caja vecina, que son cajas instaladas en comercios y almacenes de barrio.

En la **Figura 18** de la siguiente página se muestra el esquema general de las componentes que intervienen en la plataforma.

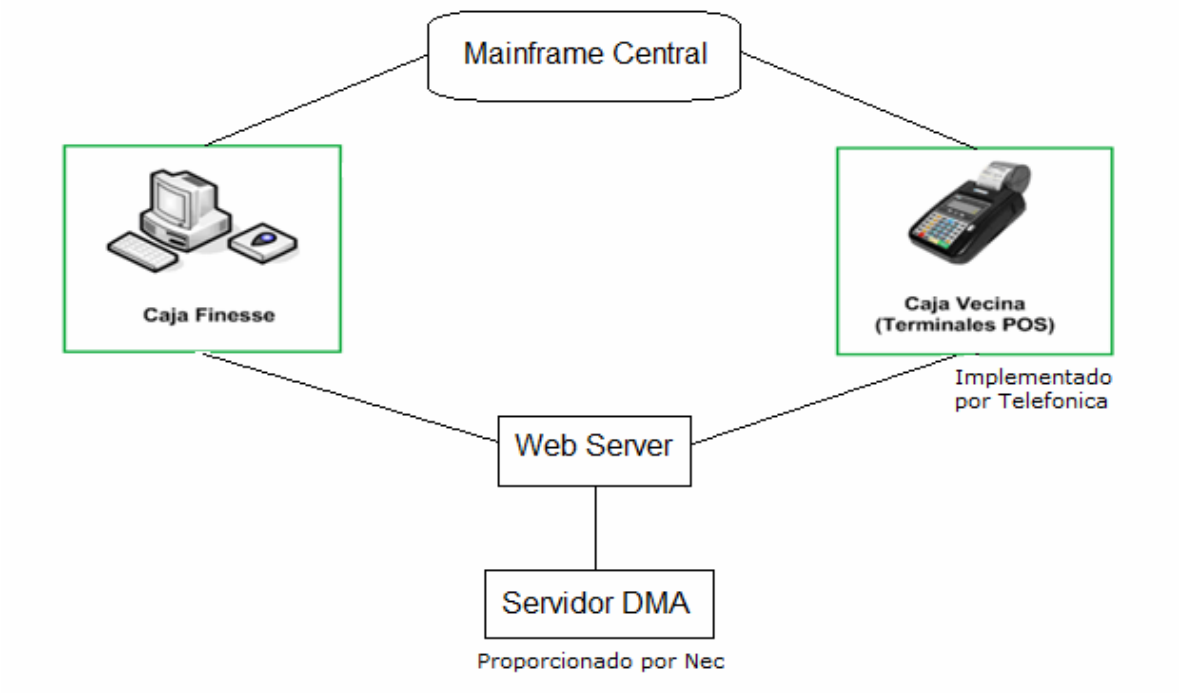

Figura 18 : Esquema general de componentes de la plataforma de validación biométrica

El servidor DMA es el que contiene el software de calce e interactúa con un web server.

Independiente del canal en que se haga la validación biométrica ésta debe ejecutar al menos 3 funciones básicas :

1) Chequeo de calidad de imagen en el dispositivo lector de huella dactilar.

2) Extracción de datos de la imagen dactilar y de la información contenida en la cédula de identidad.

3) Matching. Se realiza a través de un software, comparando dos archivos AFIS y calculando un score. Cuando este score es igual o mayor a 500, se considera que se produce calce entre huellas.

3.1.- **Uso de capturadores en caja finesse** :

El funcionamiento de la plataforma requiere de una componente de software que permita capturar huellas dactilares a nivel de estaciones clientes (caja finesse), luego las transforme a formato AFIS 378 y las envíe junto con el PDF 417 (contenido en la cédula de identidad) a los servidores DMA para su respectivo procesamiento.

En la **Figura 19** se presenta un esquema de las interfaces de caja cliente.

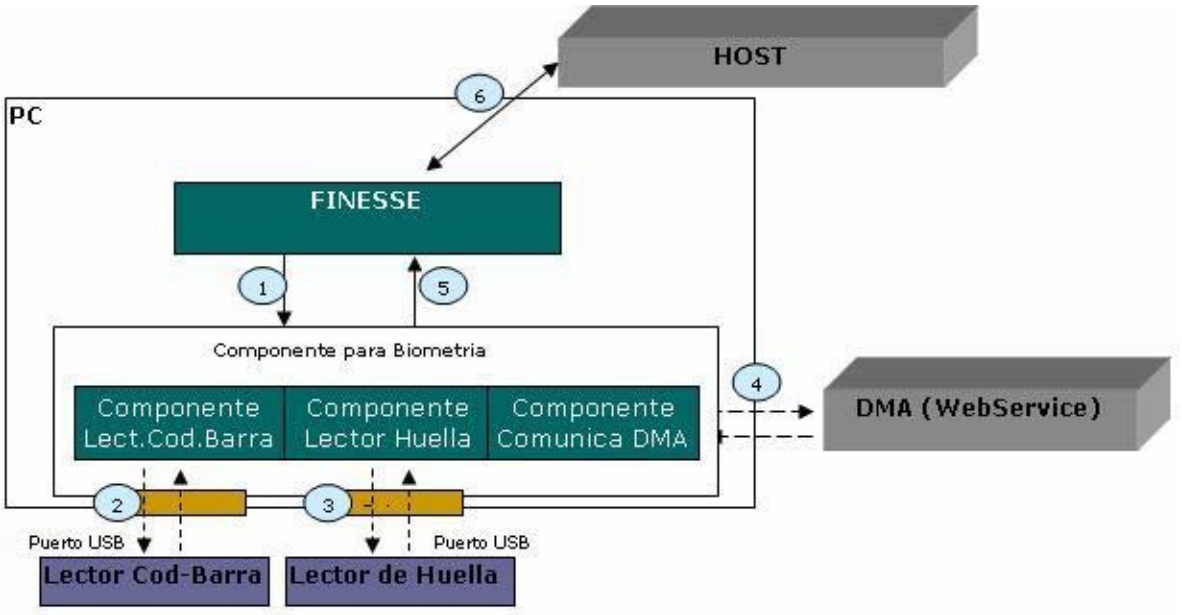

Figura 19 : Esquema general de componentes de la plataforma de validación biométrica

Interacción :

1. Finesse llama a la componente de Biometría para que realice la validación.

2. La componente obtiene la minucia de la cedula con el lector de código de barra en formato PDF 417.

3. La componente obtiene la huella dactilar del cliente.

4. La componente envía los datos al DMA para que realice la verificación.

5. La componente retorna a Finesse el resultado de la Matching.

6. Finesse, dependiendo de la respuesta, cursa la transacción a Host.

Para la captura de huellas digitales participo en la evaluación del desempeño de 2 lectores de huella digital, el primero de marca **Dermalog** modelo ZF-1 y el otro de marca **Lumidigm**. Para la lectura de cédula de identidad se probó la funcionalidad del lector de marca **Metrologic** modelo MS 1690 ya que este lector es utilizado actualmente en el banco en el sistema de recaudación de convenios y el ideal es poder utilizarlo también en este proyecto.

3.1.1.- **Lectura de cédula** :

Inicialmente se realizan pruebas conectando el lector directamente a un puerto USB. Sin embargo después de un conjunto de pruebas se determina que esta forma de conexión altera el mensaje PDF 417. Por lo que se opta por conectar éste al puerto USB con un método de emulación de dispositivo tipo COM, a través de un drive entregado por el proveedor de dicho equipo. Esta forma de conexión da resultados exitosos, permitiendo el reconocimiento del PDF 417 pero resulta incompatible con la aplicación de recaudación de convenios. Para superar este problema se opta por agregar un conector (programa interfaz) que permite leer desde la puerta COM y entregar lo capturado al drive del teclado, este esquema de captura permite la convivencia con la otra aplicaciones existente.

3.1.2.- **Lectura de huella** :

Para la lectura de huellas se prueban dos dispositivos diferentes **Dermalog y Lumidigm**, los cuales fueron preseleccionados a sugerencia de algunos proveedores del Banco. Desde el punto de vista de interfaz de programación, ambos presentan un conjunto de API´s (rutinas de interfaz de programación) que permiten capturar las huellas. En términos generales ambas interfaces están destinadas a crear una aplicación que captura una huella, el almacenamiento de ésta y la posterior comparación de esta con una nueva captura.

3.1.2.1.- **Lector Dermalog** :

La instalación del SDK (ambiente de desarrollo), esta dividida en dos, un SDK para las rutinas básicas de captura de la imagen y un segundo SDK para la manipulación de las imágenes capturadas, en especial las conversiones de formatos. Adicionalmente, este último requiere una licencia especial para la conversión a AFIS 378.

Todos los SDK dejan disponibles ejemplos de uso escritos en lenguaje C y un help con la invocación de las rutinas.

Durante el desarrollo, se logra invocar las rutinas de captura de huellas y las de control de algunos parámetros como el brillo, contraste, etc. Sin embargo, el proveedor indicó que dichos parámetros no deben ser modificados.

En la segunda etapa del desarrollo, la conversión a AFIS 378, sólo se logra la conversión con un ejecutable separado, lo que implica que la aplicación de captura resulta más compleja producto que el resultado debe pasar por un almacenamiento adicional y un mecanismo de control de término del ejecutable.

El desarrollo con las rutinas Dermalog es complejo y la aplicación final es difícil de estabilizar, adicionalmente, la documentación indica que se requiere de Windows XP service pack 2.

3.1.2.2.- **Lector Lumidigm** :

La instalación del SDK (ambiente de desarrollo), deja disponible ejemplos de uso escritos en lenguaje C y documentos PDF con la invocación de las rutinas.

Posee una interfaz dividida en rutinas básicas que facilitan la captura, permitiendo el control de algunos parámetros como brillo y contraste, también posee rutinas de alto nivel que realizan la captura de imágenes en forma automática. El formato natural de las minucias es AFIS 378, por lo que no requieren una transformación adicional.

En conclusión, el desarrollo con las rutinas Lumidigm es expedito y la aplicación final es estabilizada rápidamente. Adicionalmente la documentación indica que requiere de Windows XP service pack I.

3.1.3.- **Conclusiones** :

Lectura de cédula

La solución basada en conectar el lector, vía USB con emulación COM, opera en forma satisfactoria para la lectura del PDF 417. El agregar el emulador "COM interfaz humana", deja disponible la compatibilidad con las aplicaciones existentes por lo que el lector Metrologic puede operar en la aplicación de caja en forma satisfactoria.

Lectura de huella

Después de utilizar ambas interfaces se puede llegar a las siguientes conclusiones :

1. Las API's de **LUMIDIGM** son más fáciles de integrar y utilizar desde el punto de vista del desarrollo de conectores.

2. La documentación asociada al KIT de desarrollo de **LUMIDIGM** es más explícita que la del proveedor del dispositivo **DERMALOG**.

3. La utilización del KIT **LUMIDIGM** no requiere de licencias adicionales para la conversión puesto que trabajan en forma nativa con AFIS 378.

4. **LUMIDIGM** requiere sólo XP service pack I.

Ante la evidencia de lo expuesto, se opta por utilizar el dispositivo **LUMIDIGM.**

3.2.- **Análisis funcional caja finesse** :

Los terminales de caja que no cuenten con los dispositivos biométricos (lector de código de barra y escáner biométrico) instalados, continuarán operando con el ingreso manual del Rut del beneficiario. El sistema de caja finesse automáticamente debe reconocer si los dispositivos se encuentran instalados por lo que no se requieren acciones adicionales.

En caso que el terminal de caja cuente con los dispositivos biométricos instalados, por "default" se debe solicitar validación biométrica del beneficiario o apoderado. Si se presenta un beneficiario que no pueda ser validado biométricamente, ya sea por que posee el modelo de cédula de identidad antiguo o la calidad de su huellas dactilares no permite su lectura o incluso por que el beneficiario está inhabilitado físicamente para ser validado, el cajero debe marcar la opción de uso de la transacción sin validación biométrica (ver **Figura 20**) y así pasar a la opción de ingreso manual del Rut.

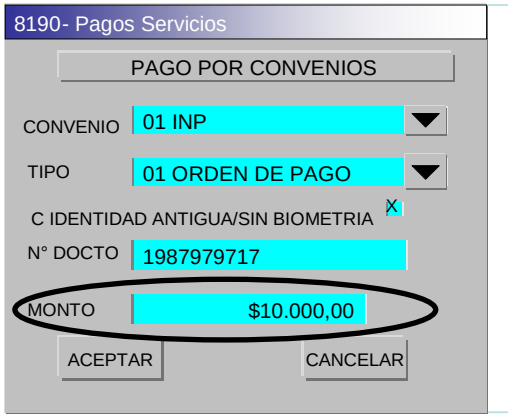

Figura 20 : Pantalla finesse con opción de marca manual (sin validación biométrica)

Si el beneficiario no presenta impedimentos para ser validado biométricamente, el cajero debe capturar el código de barra que aparece en la parte posterior de la cédula de identidad con la pistola lectora de código de barras (**Figura 21 y Figura 22**).

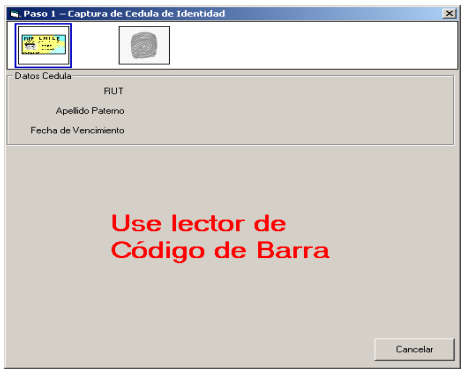

Figura 21 : Solicitud de lectura de cédula de identidad **Figura 22** : Uso de lector de código de barras

El sistema de caja finesse captura el Rut, el apellido paterno del cliente y la información del dedo que debe ser escaneado. Una vez identificado el dedo a leer, el cajero le solicita al cliente que ponga el dedo sobre el scanner biométrico.

Figura 23 : Solicitud de lectura de huella digital, el dedo a leer es el indicado en la cédula

El scanner biométrico valida que la lectura de la huella dactilar posea la calidad mínima para la comparación con la minucia. Sólo se tienen tres opciones para capturar una huella de calidad mínima. En caso que no se alcance la calidad mínima en las tres opciones se cancela la transacción, debiendo reingresar la txn si se desea insistir.

Figura 24 : Pantalla de verificación de calce

El sistema de caja envía la información de la cédula y huella dactilar, para que centralizadamente se verifique que ambos datos coincidan. Si la información de la huella y

cédula coinciden, con el dato del Rut (capturado con la pistola de código de barras al leer la cédula) se valida si el cliente presenta algún pago vigente, en caso de ser así, se presenta en pantalla los pagos disponibles del cliente (ver **Figura 25**). En caso que no existan pagos vigentes se debe indicar con un mensaje en pantalla.

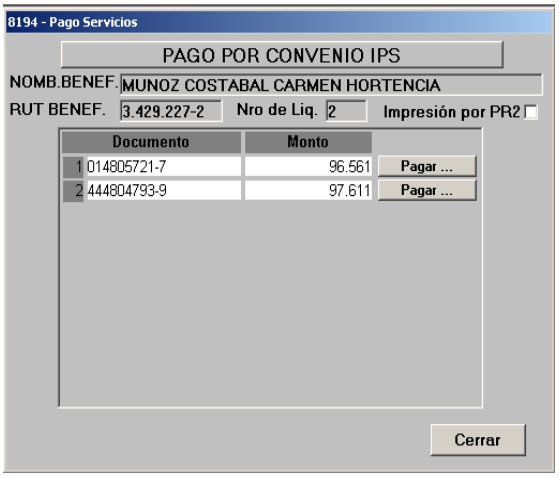

Figura 25 : Pagos disponibles una vez que la validación biométrica ha sido exitosa

En caso que la información de la huella dactilar y la cédula de identidad no coincidan, se rechaza el pago inmediatamente por fallo en la validación biométrica. El cajero puede continuar con el pago, pero debe extremar medidas de seguridad ya que el rechazo biométrico representa un antecedente a considerar. Se debe reingresar la transacción en el sistema de caja finesse y marcar la opción de validación sin biometría.

3.3.- **Análisis funcional caja vecina** :

Para incorporar la nueva funcionalidad, es necesario implementar las siguientes modificaciones al sistema actual de comunicación.

Modelo de comunicaciones :

Al modelo de comunicación entre POS y Switch se incorpora un nuevo enlace que es el Servidor Centralizado DMA, que es el encargado de validar la consistencia de los algoritmos rescatados de la cédula de identidad y de la lectura biométrica dactilar.

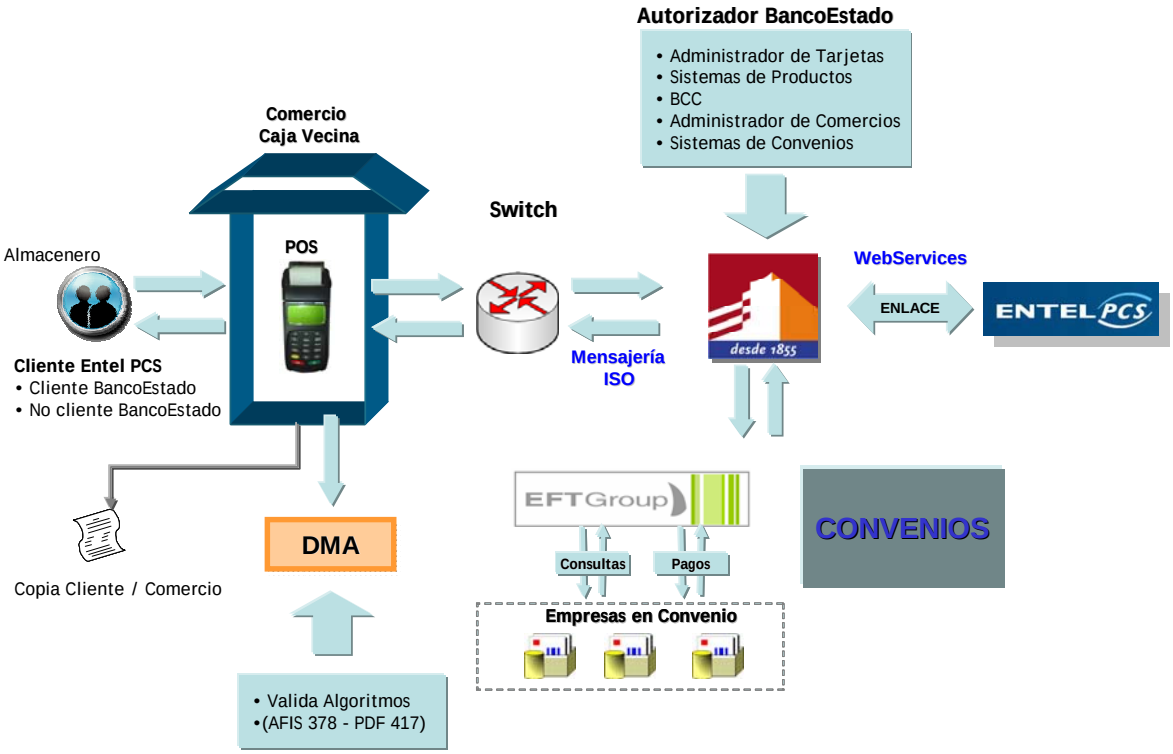

Figura 26 : Nuevo modelo de comunicación entre POS y Switch, se agrega nuevo enlace con DMA

Descripción de transacción de beneficios IPS :

Esta transacción esta destinada a clientes o no clientes de Bancoestado, específicamente a aquellas personas que sean beneficiarios de algún tipo de pensión otorgada por IPS. Los pagos de los beneficios pueden ser recepcionados por el titular del beneficio o bien su apoderado.

Modelo general de operación para el proceso de autenticación de clientes IPS mediante calce de imágenes dactilares :

El modelo de operación de IPS opera a través del flujo de comunicaciones que tiene caja vecina desde sus puntos de venta POS y la conexión que utilizará POS y servidor DMA.

Esta es la primera etapa de la transacción que consiste en la autenticación y para ello se hace uso de un lector de código de barras y un scanner o lector biométrico.

El procedimiento para la autenticación del cliente se hace mediante la lectura del código de barras que se encuentra en el reverso del carnet de identidad utilizando para ello un lector de código de barras, con este paso se obtiene el bloque PDF 417 lo que permite conocer el dedo y las minucias que se encuentran registradas, luego se procede a la lectura de ese dedo mediante el scanner o lector biométrico de huella digital, se obtiene así la información en formato AFIS 378.

Previa validación de la legibilidad de los datos, éstos son enviados al servidor DMA para validar la consistencia de ambos prismas dactilares.

En la **Figura 27** se grafica el proceso de validación de un cliente IPS para ciclo completo OK.

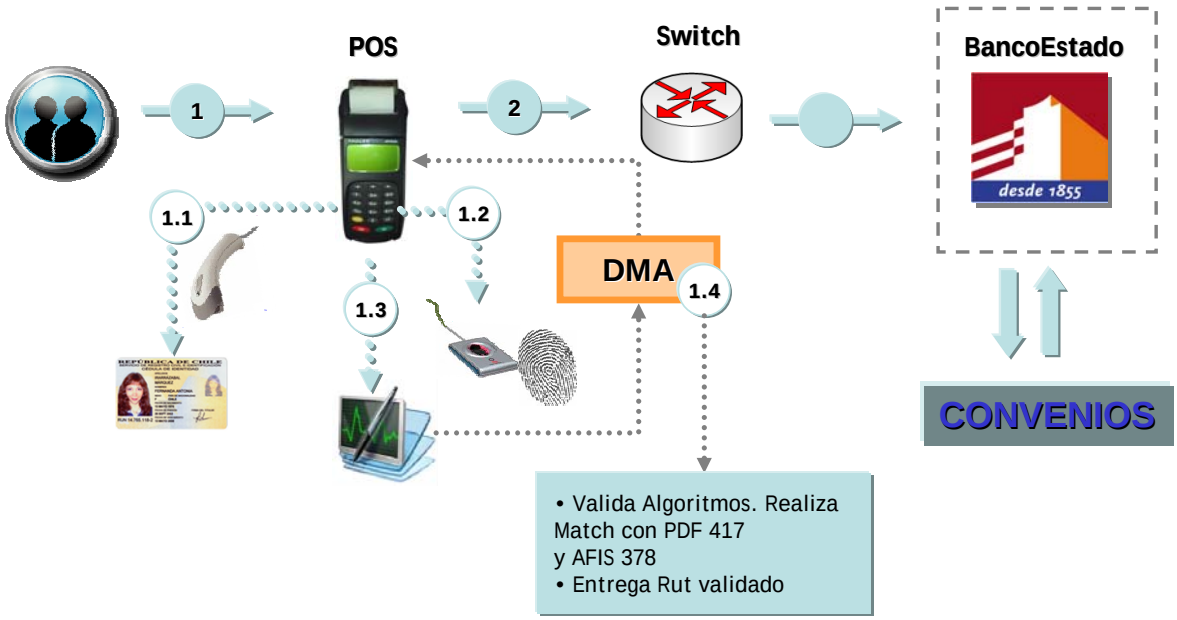

Figura 27 : Proceso de validación de un cliente IPS en canal caja vecina

Descripción funcional del proceso de autenticación de cliente IPS :

Clientes o no clientes banco verifican por caja vecina la disponibilidad de su pago.

1 Beneficiario o apoderado selecciona transacción IPS (esta transacción depende si es beneficiario o apoderado, ya que los flujos de menú son distintos).

1.1 El sistema debe leer código de barra de cédula de identidad (el sistema extrae la información del dedo que se debe validar).

1.2 El cajero debe utilizar el lector biométrico dactilar (POS indica cual es el dedo que se encuentra registrado en cédula de identidad).

1.3 Aplicación en POS :

- Valida condiciones de calidad en la lectura biométrica dactilar.
- Rescata AFIS 378 del Lector Biométrico y PDF 417 de la cédula de identidad.
- Envía los datos a un servidor centralizado DMA (Dinamic Matching Array).

1.4 Servidor centralizado DMA :

Valida y confirma la consistencia de los algoritmos rescatados de la cédula de identidad y de la lectura biométrica dactilar. De ser exitosa la validación (score resultante definido como exitoso) envía un Rut validado al POS.

2 POS envía consulta a switch con Rut devuelto por DMA (adjunta Rut autentificado)

Modelo de operación para consulta de disponibilidad de beneficio IPS :

La disponibilidad del beneficio IPS es la segunda etapa para lograr el retiro de la liquidación de IPS y consiste en informar el beneficiario si posee una o más liquidaciones por cobrar.

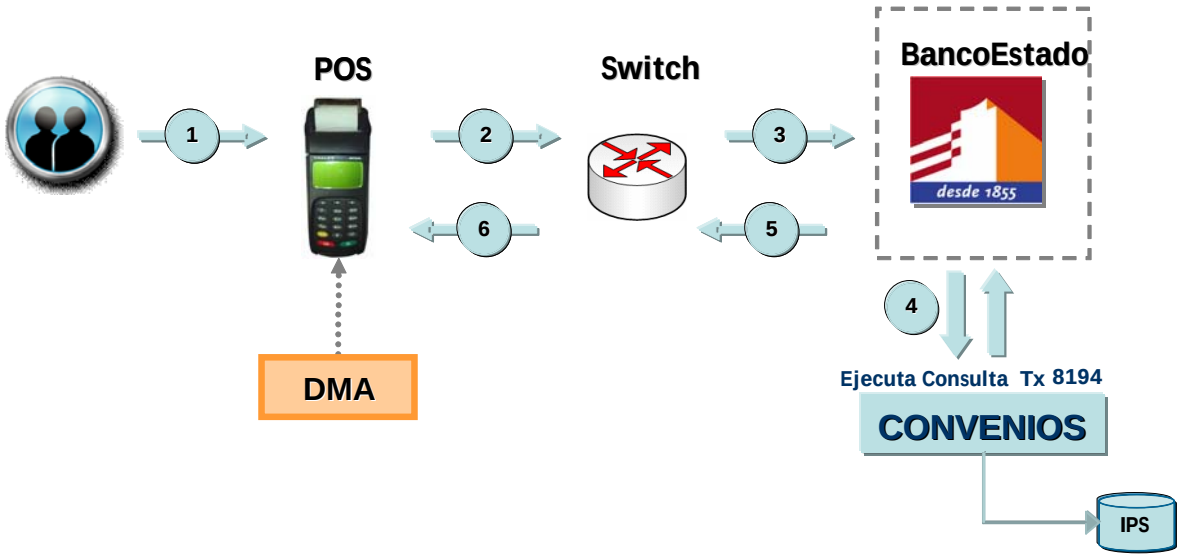

Figura 28 : Proceso de consulta de disponibilidad de beneficio IPS

Descripción general del proceso de consulta de disponibilidad de beneficio IPS

2. POS envía consulta al Switch (con Rut validado)

3. Switch envía consulta a Banco

4. Banco realiza las validaciones existentes para clientes IPS, y genera mensaje de respuesta :

Si la validación es exitosa, es decir, cliente está en los registros como beneficiario IPS y tiene monto disponible de pago, se enviarán datos del o los beneficios con su respectivo monto disponible como respuesta a la consulta de pago. Si además el Rut es apoderado, se rescatará toda la información de beneficios asociados al Rut, es decir, se enviará la información de todos los beneficiarios y beneficios asociados al Rut.

Si la validación no es exitosa, es decir, el cliente no está en los registros de beneficiario IPS, se responderá mensaje de rechazo al POS. Banco registra la transacción.

5. Banco envía la respuesta al Switch

6. Switch envía transacción al POS :

Si la respuesta del Banco indica validación es exitosa, el POS mostrará en pantalla la información del monto disponible para retiro, en el caso que el cliente tengo un solo tipo de beneficio disponible, o el detalle de todos los beneficios disponibles con su respectivo monto. Para este último caso, cada beneficio requerirá de una transacción independiente para hacerlo efectivo.

Si además es apoderado de beneficiarios con Rut, se debe desplegar una lista con el nombre del apoderado más todos los beneficiarios asociados, previa selección de uno de ellos, se muestra un listado con todos los beneficios por pagar.

Cualquiera sea la selección escogida por el cliente se requiere la validación de efectivo del comercio.

Si la respuesta del Banco indica validación no es exitosa, el POS mostrará en pantalla : mensaje de rechazo; cliente sin beneficio IPS.

Modelo de operación para pago de beneficio IPS :

El pago del beneficio es la tercera etapa y final para completar la transacción para hacer efectivo el pago de uno o más beneficios IPS.

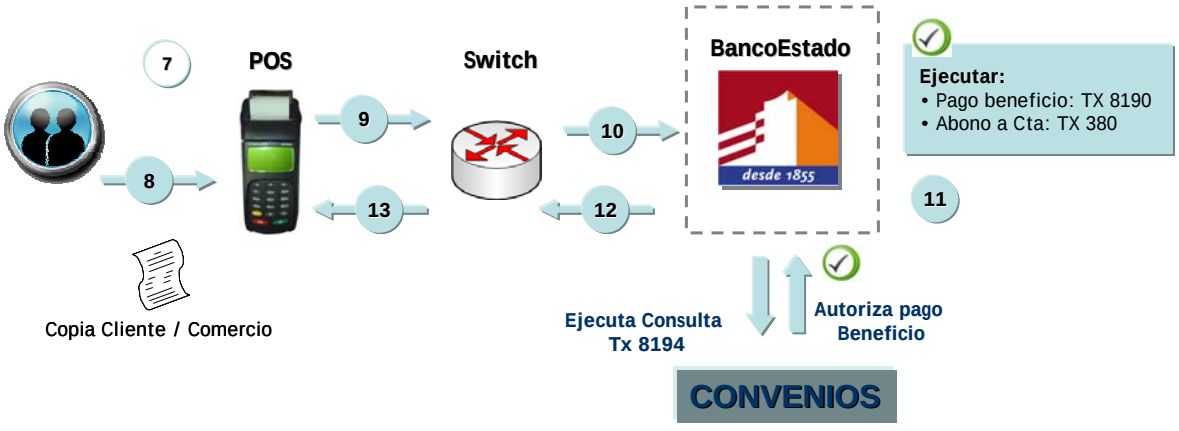

Figura 29 : Proceso de pago de beneficio IPS

Descripción general del proceso de pago de beneficio IPS :

7. El POS dará la opción al cliente de elegir sólo uno de los beneficios disponibles de pago.

8. Cliente selecciona beneficio.

9. POS envía solicitud de giro de fondos al Switch.

10. Switch envía transacción al Banco

11. Banco autoriza, registra transacción y actualiza saldos, convenio a su vez marca como entregado el beneficio seleccionado.

12. Banco envía autorización a Switch, y Switch envía autorización a POS.

13. El POS emite comprobante de pago.

Alcance : Los servicios requeridos para la consulta y pago de los convenios de IPS (incluyendo rendiciones) deben ser provistos por el sistema de convenios u otro sistema producto y no están considerados en el desarrollo del canal.

Es necesario validar el disponible de efectivo del comercio para cualquier selección escogida.

3.3.- **Análisis de casos de uso** :

El objetivo del análisis de casos de uso es el de modelar el sistema desde el punto de vista de cómo los usuarios interactúan con el sistema para lograr sus objetivos.

Nuestro modelo consiste en la identificación de cada uno de los actores del sistema, luego definimos el conjunto de casos de uso y un diagrama que indica cómo se relacionan dichos casos.

Actor	Descripción
Beneficiario	Actor principal, es quién debe ser autentificado biométricamente
Cajero	Encargado de la atención del beneficiario ya sea en caja finesse o caja vecina
Apoderado	Representante del beneficiario, debe estar definido en el sistema de convenios como apoderado oficial
Sistema de convenios	Administra los convenios suscritos por el Banco, en particular el del pago de las pensiones a los beneficiarios del IPS

A continuación se presentan los diferentes casos de uso :

Caso 1 : Validación biométrica para pago a beneficiario que puede ser validado.

Actores : Beneficiario, cajero y sistema de convenios.

Meta : Efectuar pago al beneficiario.

Precondiciones : Beneficiario porta el nuevo diseño de la cédula de identidad (con el código de barras) y su huella digital posee la calidad mínima para ser leída. Por otro la caja tiene instalados los periféricos que permiten efectuar la validación biométrica.

Resumen : Beneficiario acude a alguna sucursal del banco o a una caja vecina con el objetivo de cobrar su pensión, una vez ahí, el cajero le solicita la cédula de identidad y da inicio al proceso de validación. Lo primero es la lectura de la cédula y luego la lectura de la huella, sistema acude al sistema de convenios a buscar los pagos disponibles, si tiene pagos, el sistema los presenta en pantalla y el cajero procede a pagar al beneficiario, si no tiene pagos se informa de tal evento.

Caso de uso relacionado : Validación biométrica para pago a apoderado.

Pasos :

Acción	Respuesta del sistema
1.- Beneficiario se acerca a la caja y solicita el pago de su pensión	**2.-** Detecta que los periféricos biométricos están instalados
3.- Cajero solicita la cédula al beneficiario y utiliza el lector de código de barras para capturar la información contenida en el código de barras	**4.-** Captura el Rut, apellido paterno, dedo que debe ser escaneado y las minucias informadas en la cédula
5.- Cajero utiliza el escáner para leer la huella del dedo que indica la cédula	**6.-** Valida la calidad de la huella y envía una petición de comparación de huellas
	7.- Efectúa el proceso de comparación, calcula el score y registra la transacción
	8.- Valida que el score sea igual o mayor que el mínimo definido y envía el Rut al sistema de convenios
9.- Sistema de convenios recibe el Rut y envía todos los pagos disponibles para el beneficiario	**10.-** Muestra en pantalla todos los pagos disponibles
11.- Cajero paga al beneficiario	

Postcondiciones : Se almacena la fecha y hora de la transacción (comparación de minucias), se guarda además la caja en que se hizo la transacción, si ésta fue exitosa o no y cuál fue el score que se obtuvo, esto con el objeto de generar informes de desempeño y gestión.

Caso 2 : Validación biométrica para pago a apoderado que puede ser validado.

Actores : Apoderado, cajero y sistema de convenios.

Meta : Efectuar pago al apoderado.

Precondiciones : Apoderado porta el nuevo diseño de la cédula de identidad, su huella digital posee la calidad mínima para ser leída y está definido en el sistema de convenios como apoderado de uno o más beneficiarios del IPS. Por otro la caja tiene instalados los periféricos que permiten efectuar la validación biométrica.

Resumen : Apoderado acude a alguna sucursal del banco o a una caja vecina con el objetivo de cobrar la pensión de el o los beneficiarios que lo han designado como su apoderado, una vez ahí, el cajero le solicita la cédula de identidad y da inicio al proceso de validación. Se leen la cédula y la huella, luego el sistema acude al sistema de convenios a buscar los beneficiarios asociados al apoderado y los pagos disponibles que serán entregados al apoderado.

Caso de uso relacionado : Validación biométrica para pago a beneficiario.

Pasos :

Acción	Respuesta del sistema
1.- Apoderado se acerca a la caja y solicita el pago de la pensión de su(s) pupilo(s)	**2.-** Detecta que los periféricos biométricos están instalados
3.- Cajero solicita la cédula al apoderado y utiliza el lector de código de barras para capturar la información contenida en el código de barras	**4.-** Captura el Rut, apellido paterno, dedo que debe ser escaneado y las minucias informadas en la cédula
5.- Cajero utiliza el escáner para leer la huella del dedo que indica la cédula	**6.-** Valida la calidad de la huella y envía una petición de comparación de huellas
	7.- Efectúa el proceso de comparación, calcula el score y registra la transacción
	8.- Valida que el score sea igual o mayor que el mínimo definido y envía Rut al sistema de convenios
9.- Sistema de convenios recibe el Rut y envía todos los beneficiarios asignados al apoderado y todos pagos disponibles para esos beneficiarios	**10.-** Muestra en pantalla todos beneficiarios y los pagos disponibles para ellos
11.- Cajero paga al beneficiario	

Postcondiciones : Sistema guarda la fecha y hora de la transacción (comparación de minucias), guarda además la caja en que se hizo la transacción, si ésta fue exitosa o no y cuál fue el score que se obtuvo, esto con el objeto de generar informes de desempeño y gestión.

Caso 3 : Validación biométrica para pago a beneficiario con mala calidad de huella.

Actores : Beneficiario, cajero, sistema de convenios.

Meta : Efectuar pago al beneficiario que no puede ser validado biométricamente ya que su huella es de mala calidad.

Precondiciones : Beneficiario porta el nuevo diseño de la cédula de identidad (con el código de barras). Caja tiene instalados los periféricos que permiten efectuar la validación biométrica.

Resumen : Beneficiario acude a alguna sucursal del banco o a una caja vecina con el objetivo de cobrar su pensión, una vez ahí, el cajero le solicita la cédula de identidad y da inicio al proceso de validación. Se lee la cédula y luego se lee la huella.

Pasos :

Acción	Respuesta del sistema
1.- Beneficiario se acerca a la caja y solicita el pago de su pensión	**2.-** Detecta que los periféricos biométricos están instalados
3.- Cajero solicita la cédula al beneficiario y utiliza el lector de código de barras para capturar la información impresa en el código de barras	**4.-** Captura el Rut, apellido paterno, dedo que debe ser escaneado y las minucias informadas en la cédula
5.- Cajero utiliza escáner para leer la huella del dedo que indica la cédula	**6.-** No es capaz de validar a huella y solicita un segundo intento de lectura
7.- Cajero intenta leer por segunda vez la huela	**8.-** No es capaz de validar a huella y solicita un tercer intento de lectura
9.- Cajero intenta leer por tercera vez la huela	**10.-** No es capaz de validar, por tercera vez, la huella y aborta el proceso de validación biométrica
11.- Cajero marca opción de pago sin validación biométrica	

Postcondiciones : Beneficiario tendrá siempre problemas para ser validado. Se podrá evaluar la posibilidad de levantar un requerimiento de mantención al sistema que permita registrar a los beneficiarios con mala calidad de huella.

Caso 4 : Validación biométrica cuando no coinciden las huellas.

Actores : Beneficiario y cajero.

Meta : Rechazo del pago por no existencia de validación biométrica.

Precondiciones : Beneficiario porta el nuevo diseño de la cédula de identidad (con el código de barras). Caja tiene instalados los periféricos que permiten efectuar la validación biométrica.

Resumen : Beneficiario acude a alguna sucursal del banco o a una caja vecina con el objetivo de cobrar su pensión, una vez ahí, el cajero le solicita la cédula de identidad y da inicio al proceso de validación. Se lee la cédula y luego se lee la huella, en este caso no se alcanzan a rescatar los pagos que tiene disponibles el beneficiario ya que no existe coincidencia entre la huella dactilar y la huella leída en la cédula.

Pasos :

Acción	Respuesta del sistema
1.- Beneficiario se acerca a la caja y solicita el pago de su pensión	**2.-** Detecta que los periféricos biométricos están instalados
3.- Cajero solicita la cédula al beneficiario y utiliza el lector de código de barras para capturar la información impresa en el código de barras	**4.-** Captura el Rut, apellido paterno, dedo que debe ser escaneado y las minucias informadas en la cédula
5.- Cajero utiliza escáner para leer la huella del dedo que indica la cédula	**6.-** Valida la calidad de la huella y envía una petición de comparación de huellas
	7.- Efectúa el proceso de comparación, calcula el score y registra la transacción
	8.- Verifica que el score es menor que el mínimo definido y acusa rechazo en la validación biométrica
9.- Cajero informa al beneficiario que no podrá efectuar el pago de la pensión por no existir coincidencia entre la cédula y la huella digital	

Postcondiciones : Queda a criterio de la jefatura de la sucursal la posibilidad de pago manual aun existiendo rechazo en validación biométrica.

En la siguiente página se encuentra la **Figura 30** con el diagrama de los actores y casos de uso descritos anteriormente

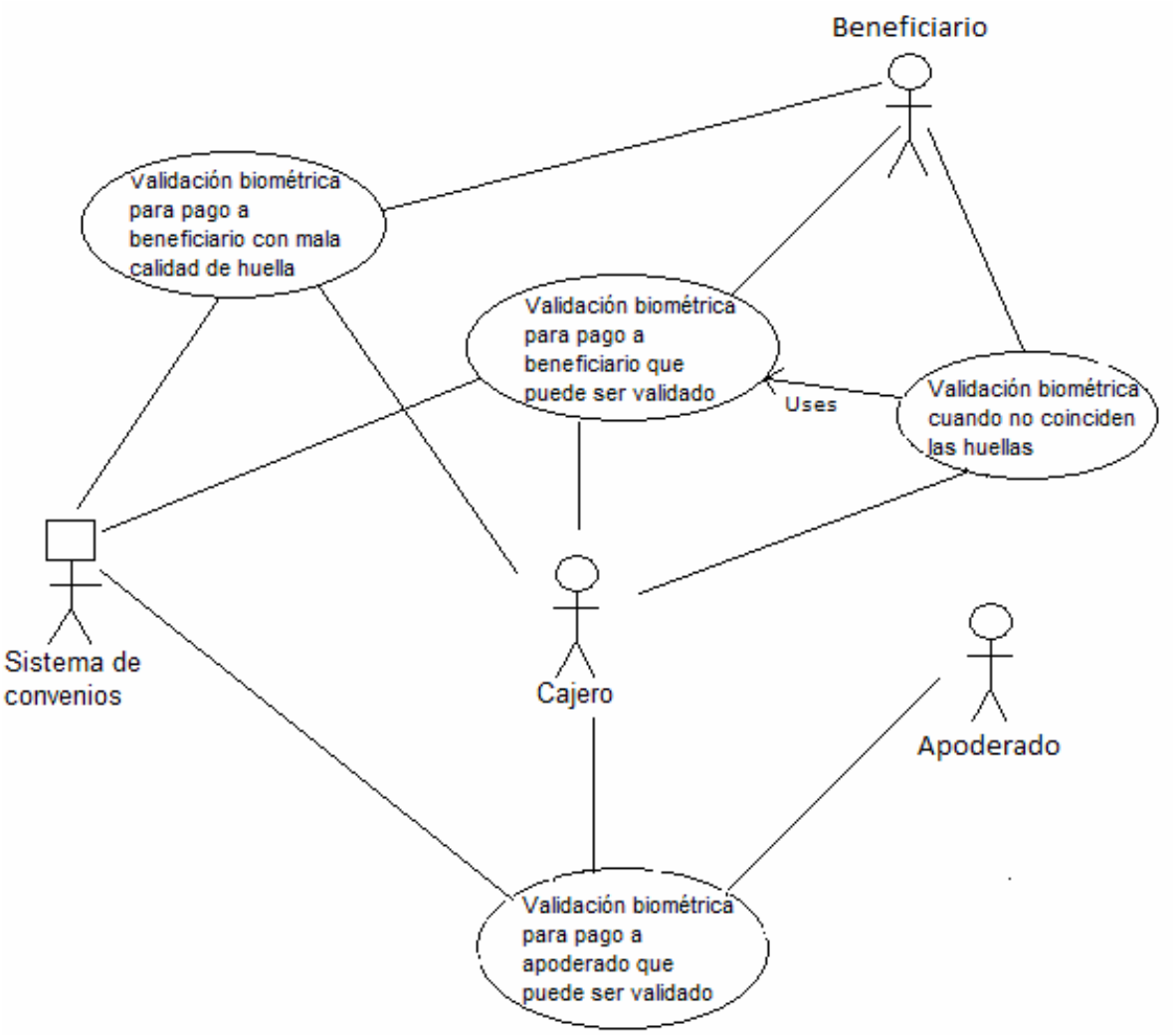

Figura 30 : Diagrama de casos de uso

3.5.- **Criterios de aceptación del sistema** :

En esta sección se define los criterios a evaluar una vez realizadas las pruebas definidas en el protocolo de aceptación definido para el sistema el cual será descrito en el capítulo de pruebas del presente trabajo.

La ejecución del protocolo de aceptación constituye el medio objetivo para la aceptación de una aplicación ó módulo funcional.

El protocolo de aceptación debe permitir validar todas las características de la aplicación tanto a nivel funcional (que se puedan realizar los casos de uso previstos), como características

no funcionales (por ejemplo, performance, compatibilidad con los estándares que correspondan, robustez, capacidad, etc.).

Se definen 3 tipos de problemas según la gravedad de los mismos.

Problemas tipo A :

Se define como falla tipo A, a toda falla bloqueante a nivel funcional, tal como inconsistencia en transacciones, caída del sistema, falta de implementación o falla en la funcionalidad principal, degradación grave de performance.

Problemas tipo B :

Se define como falla tipo B a toda falla que afecte puntualmente a una función secundaria pero que no impide que se lleven a cabo normalmente las funciones centrales del sistema. Ejemplo de fallas tipo B son : falla en una operación de búsqueda accesoria y degradación de performance menor a 10% de la especificada.

Problemas tipo C :

Se define como falla tipo C a toda falla menor que no afecta el funcionamiento general del sistema. Se trata de problemas estéticos, errores de ortografía, formato de impresión, etc.

Se establece entonces el siguiente, como criterio de aceptación :

Criterio para la aceptación del Sistema :

El sistema sobre el que se decidirá la aceptación será evaluado a través de la ejecución del protocolo de aceptación, tal como lo descrito en el punto anterior.

Se dará por satisfactoria la versión de producto si no supera el siguiente mapa de fallas :

Tipos de Falla	Cantidad
A	No deberá haber defectos tipo A abiertos.
B	Podrá haber defectos tipo B abiertos, pero sin superar el 5% de los puntos de función.
C	Podrá haber defectos tipo C abiertos, pero sin superar el 10% de los puntos de función.

Los pendientes tipo B y C detectados quedarán asentados en el protocolo de aceptación donde se establecerá la fecha de compromiso de solución de los mismos.

Aceptación final :

La aceptación final de la plataforma tiene lugar una vez realizadas las pruebas definidas en el protocolo de aceptación. Para la aceptación final pueden tenerse en cuenta factores como la información de fallas presentadas (no deberán existir fallas pendientes de solución), información de penetración de uso del sistema. (verificar la adopción del sistema en las tareas para las que fue creado). Los indicadores de uso, así como los umbrales de nivel de penetración (nulo, bajo, satisfactorio y sobresaliente) o cualquier otro factor que determine la aceptación del sistema, se definirán y volcarán en el protocolo de aceptación, registrándose sus valores con intervalos definidos.

4.- **Arquitectura** :

Para dar contexto y soporte al desarrollo de la plataforma biométrica, se adjunta la definición conceptual de la solución en la cual muestra la forma en que se pretende realizar la comunicación entre los canales y la infraestructura servidora, junto con definir la mensajería a utilizar en todo el proceso.

La solución conceptual que se propone viene expresada en el siguiente diagrama :

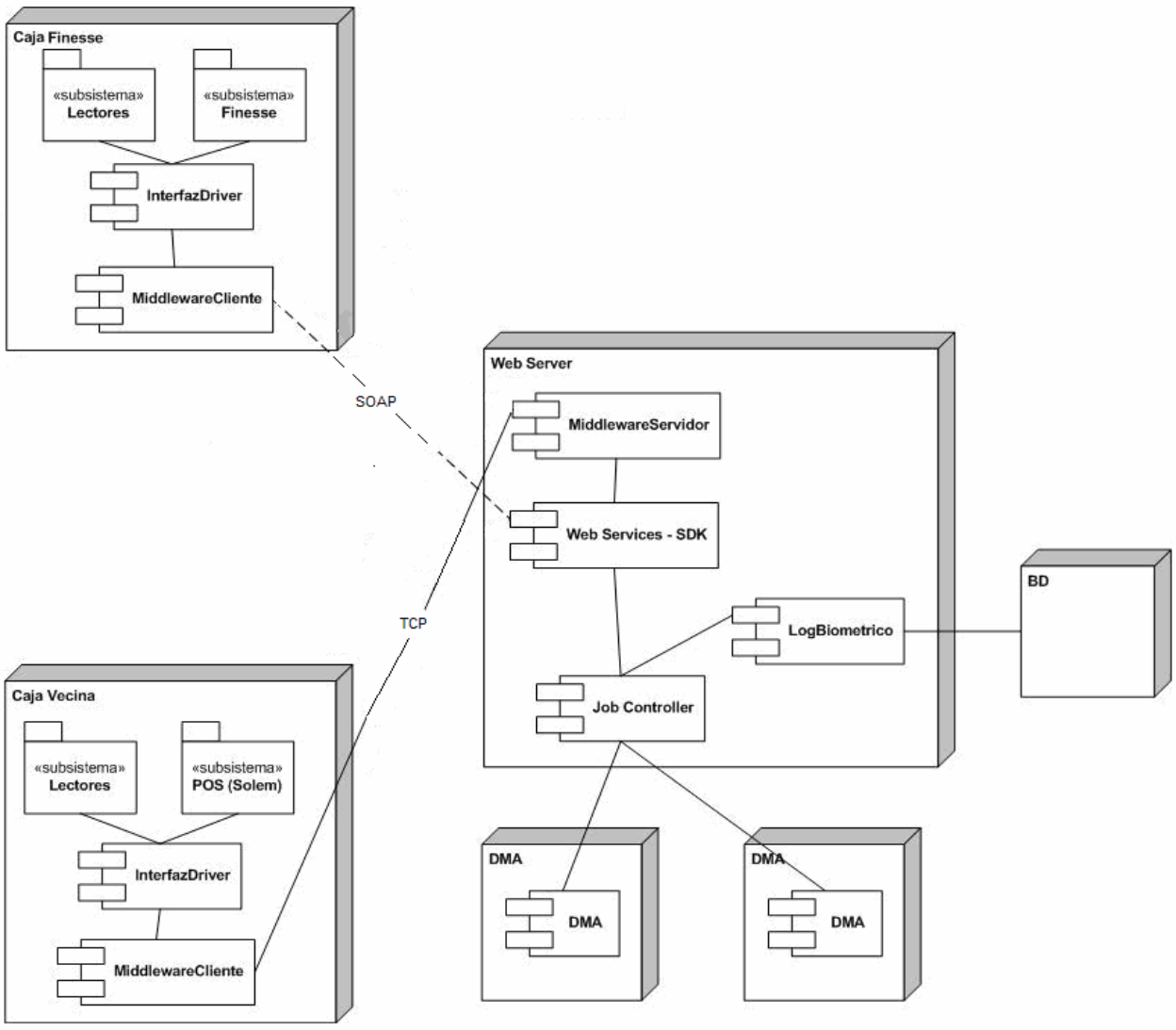

Figura 31 : Arquitectura del sistema de validación biométrica

4.1.- **Componentes de la solución** :

4.1.1.- **Software básico** :

- Windows 2003 para servidores.
- SQL 2005 para motor de datos.

4.1.2.- **Software desarrollado a medida** :

- Listener http, el cual denominaremos en este documento como MiddlewareServidor.

- Integrador cliente, denominado en este documento como MiddlewareCliente (Especificado en etapa de diseño, sólo para el ámbito de caja finesse).

- Integrador para caja vecina, denominado en el documento como InterfazDriver.

- Integrador para caja, denominado en el documento como InterfazDriver (Especificado en etapa de diseño, sólo para el ámbito de caja finesse).

- Conversor AFIS, componente que surge de una personalización del Job Controller.

4.1.3.- **Software provisto por NEC** :

- Consola de administración.
- Developer (SDK) para web services de integración.

4.2.- **Deploy de componentes en servidores** :

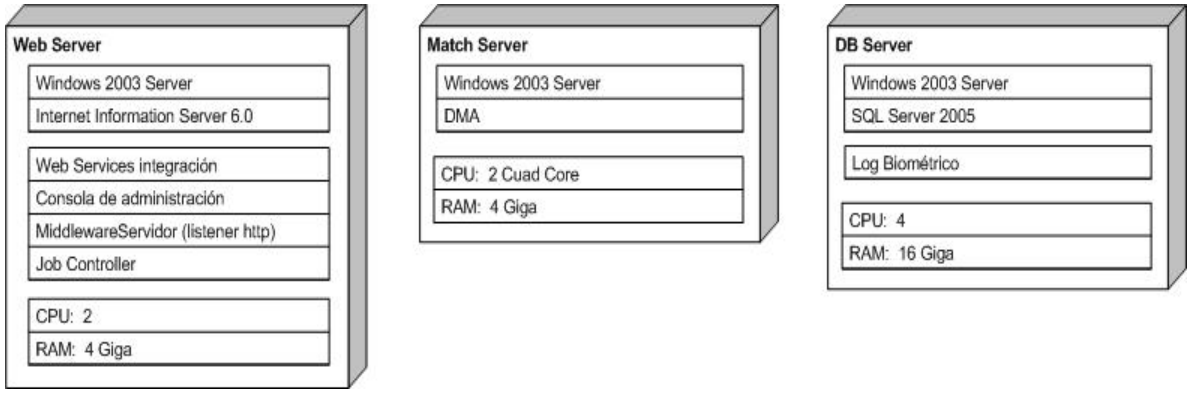

Figura 32 : Despliegue de componentes en servidores

4.3.- **Deploy de componentes en canales** :

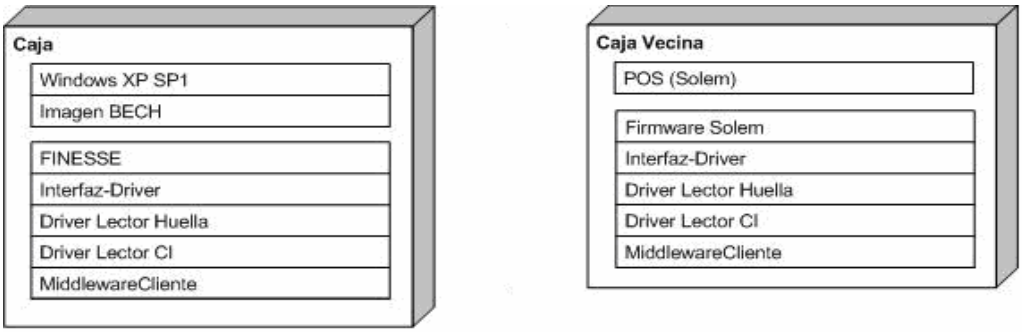

Figura 33 : Despliegue de componentes en canales

4.4.- **Flujos De Información** :

4.4.1.- **Proceso de validación** :

Dentro de este proceso participan : Los canales, integradores en los canales, integrador en el servidor (listener http), job controller, matching y la base de datos para el log biométrico.

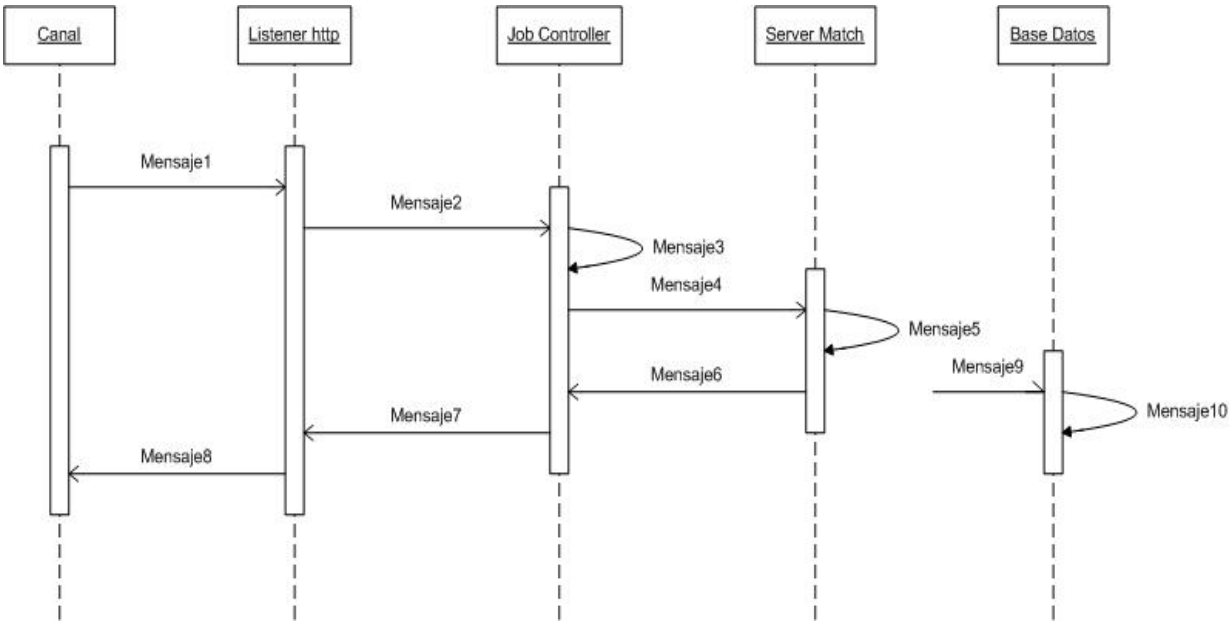

Figura 34 : Mensajería del proceso de validación

Datos y argumentos en cada llamada :

- Mensaje 1 y 2 : Llamada desde el canal al Job Controler

- Mensaje 3 : Conversión de norma
- Mensaje 4 : Solicitud de validación al servidor de match
- Mensaje 5 : Proceso de validación
- Mensaje 6, 7 y 8 : Respuesta de la validación
- Mensaje 9 : Proceso asíncrono de registro de log biométrico

4.4.2.- **Proceso De Validación caja finesse** :

Proceso detallado del canal caja, los componentes que participan en este proceso son : Finesse, Interfaz-Driver, Middleware-Cliente, Middleware-Servidor (listener http), Job Controller, Servidor de match y Log Biométrico (base de datos)

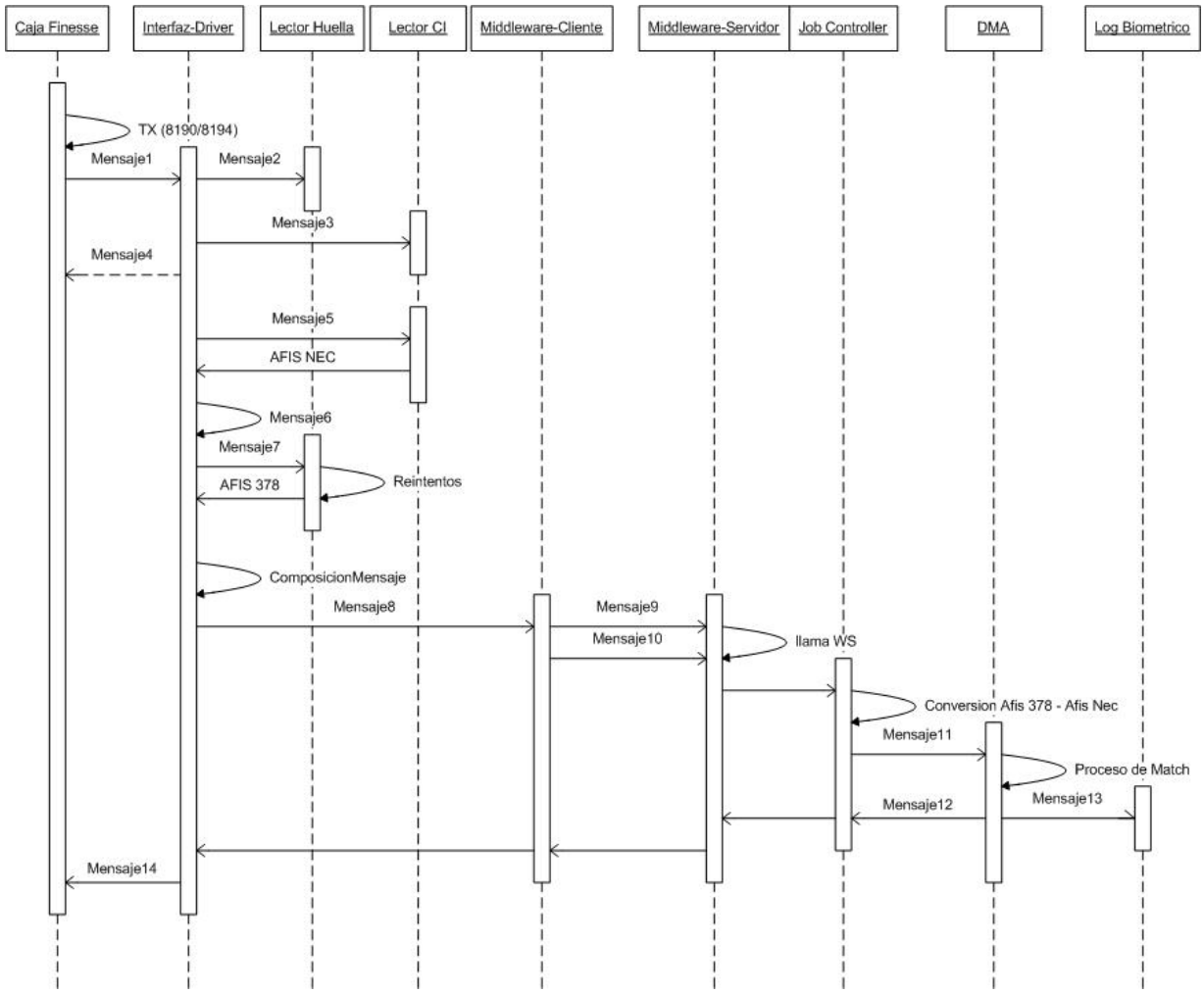

Figura 35 : Mensajería del proceso de validación en caja finesse

Datos y argumentos en cada llamada :

- Mensaje 1 : Pasa el control a la componente *Interfaz-Driver*
- Mensaje 2 : Valida que esté el dispositivo lector de huella
- Mensaje 3 : Valida que esté el dispositivo lector de CI
- Mensaje 4 : Retorna el control si no hay dispositivos
- Mensaje 5 : Lectura del CI
- Mensaje 6 : Procesa las condiciones establecidas en la información del CI, ej: que dedo debe usarse
- Mensaje 7 : Lectura huella, efectúa reintentos si la calidad de la lectura no es óptima
- Mensaje 8 : Interfaz-Driver genera y pasa mensaje a enviar a la componente MiddlewareCliente. El mensaje se compone de :

  - Header Banco
  - IP_Origen
  - AFIS_378
  - AFIS_NEC

- Mensaje 9 : Llamado al listener tcp, usando estándar ISO en la mensajería
- Mensaje 10 : Llamado a los WS, usando SOAP
- Mensaje 11 : *Job Controller* compone mensaje con la conversión del código AFIS_378 a AFIS_NEC(2) y lo envia al servidor de match, mensaje :

  - Header Banco
  - IP_Origen
  - AFIS_378
  - AFIS_NEC
  - AFIS_NEC(2)

- Mensaje 12 : El servidor de match compone mensaje con el resultado de la verificación Biométrica y se los entrega al *Job Controller*. mensaje :

  - Header Banco
  - IP_Origen
  - SCORE
  - SI/NO
  - CRC

- Mensaje 13 : El servidor de match compone mensaje con el resultado de la verificación Biométrica y genera una llamada asíncrona al sistema *Log Biométrico*. mensaje :

- HeaderBanco
- IP_Origen
- AFIS_378
- AFIS_NEC
- AFIS_NEC(2)
- SCORE
- SI/NO
- CRC

- Mensaje 14 : Retorna el control a Finesse

4.4.3.- **Proceso de validación caja vecina** :

Proceso detallado del caja vecina, los componentes que participan en este proceso son : software POS Caja Vecina, Interfaz-Driver, Middleware-Cliente, Middleware-Servidor (listener http), Job Controller, Servidor de match y Log Biométrico (base de datos).

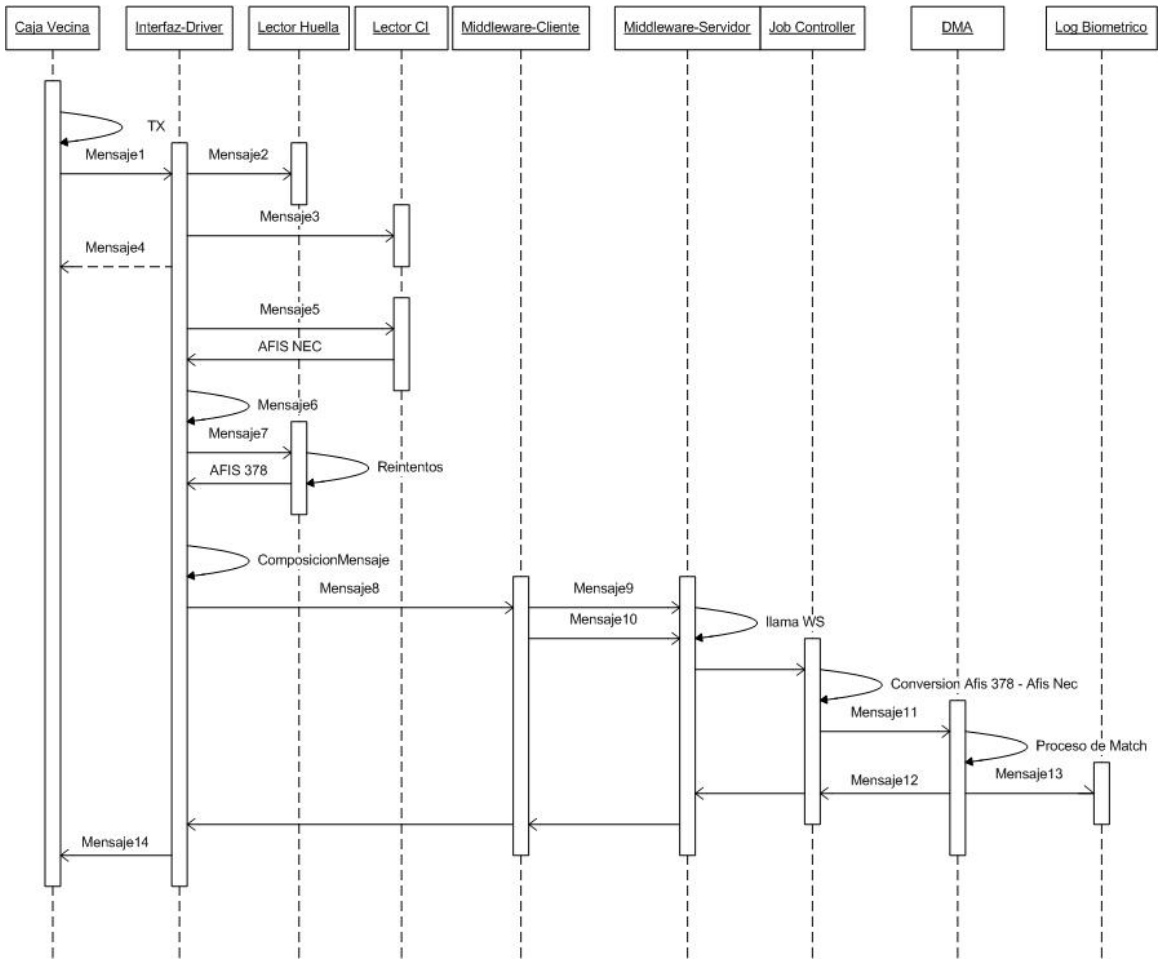

Figura 36 : Mensajería del proceso de validación en caja vecina

Datos y argumentos en cada llamada :

- Mensaje 1 : Pasa el control a la componente Interfaz-Driver.
- Mensaje 2 : Valida que este el dispositivo lector de huella.
- Mensaje 3 : Valida que este el dispositivo lector de CI.
- Mensaje 4 : Retorna el control si no hay dispositivos.
- Mensaje 5 : Lectura del CI.
- Mensaje 6 : Procesa las condiciones establecidas en la información del CI, ejemplo : dedo que debe usarse.
- Mensaje 7 : Lectura huella, efectúa reintentos si la calidad de la lectura no es óptima.
- Mensaje 8 : Interfaz-Driver genera y pasa mensaje a enviar a la componente MiddlewareCliente. Mensaje :

  - Header Banco
  - IP_Origen
  - AFIS_378
  - AFIS_NEC

- Mensaje 9 : Llamado al listener tcp, usando estándar ISO en la mensajería.
- Mensaje 10 : Llamado al web server, usando SOAP.
- Mensaje 11 : Job Controller compone mensaje con la conversión del código AFIS_378 a AFIS_NEC(2) y lo envía al servidor de match. Mensaje :

  - Header Banco
  - IP_Origen
  - AFIS_378
  - AFIS_NEC
  - AFIS_NEC(2)

- Mensaje 12 : El servidor de match compone mensaje con el resultado de la verificación biométrica y se los entrega al Job Controller. Mensaje:

  - Header Banco
  - IP_Origen
  - SCORE
  - SI/NO
  - CRC

- Mensaje 13 : El servidor de match compone mensaje con el resultado de la verificación Biométrica y genera una llamada asíncrona al sistema Log Biométrico. Mensaje :

- HeaderBanco
- IP_Origen
- AFIS_378
- AFIS_NEC
- AFIS_NEC(2)
- SCORE
- SI/NO
- CRC

- Mensaje 14 : Retorna el control el software de caja vecina.

4.5.- **Log biométrico** :

Es el registro de las transacciones efectuadas en un proceso de validación biométrica que tiene por objeto hacer una consulta posterior, ya sea para confeccionar estadísticas, para medir desempeños o por necesidades de auditoría.

En el Log Biométrico se almacenan todas las verificaciones de identidad realizados por el Banco y se pueden consultar mediante consultas y reportes.

El Log biométrico es generado en forma asíncrona, de modo de evitar contención.

4.5.1.- **Datos del Log Biométrico** :

Numero Rut cliente.
Digito verificador Rut cliente.
Código de oficina.
Número de terminal.
Código de canal.
Código de la transacción.
Fecha transacción biométrica.
Hora transacción biométrica.
Identificador de estación de trabajo origen de la transacción.
Plantilla de minucias en formato AFIS 378 (de la captura en vivo).
Bloque PDF 417 (de la cédula de identidad).
Valor del Resultado : Coincidencia / No Coincidencia / Error.
Identificador único de la transacción biométrica, generado por DMA.
Score transacción biométrica.
Fecha de la operación.
Plantilla de minucias NEC (PC1) obtenida de la conversión de la plantilla AFIS 378.

4.6.- **Integración** :

La integración de la solución biométrica entregada por NEC con los distintos canales involucrados está resuelta con el uso de un SDK (software developer kit) para construcción de web services que recibe información desde la punta (canal) para que sea procesada por el servidor de match y retornada al origen. Cabe destacar que la integración y uso del SDK está sólo delimitada a la componente servidora de la solución y no hay desarrollos de validación o match locales en los diferentes canales.

4.6.1.- **Definición de los procesos a exponer en los web service** :

Proceso de captura de información.

4.6.2.- **Seguridad en los web service** :

Implementado con el uso de certificados digitales

4.6.3.- **Universo de periféricos en los canales** :

Caja Vecina = 46
Caja Finesse = 900 +

Total de cajas = 946

5.- **Diseño** :

La solución biométrica se debe hacer cargo de la necesidad de integrar 2 canales : Caja Finesse y Caja Vecina (POS). Esta solución se compone de una parte cliente, encargada de recolectar la información de minucias en la punta y una parte servidora encargada del proceso de comparación de esa información.

Los canales antes señalados comparten conceptualmente los requerimientos de módulos a desarrollar para lograr el funcionamiento de la validación biométrica por lo cual la solución en el cliente se modularizó entregando como resultado dos componentes; el primero denominado "Interfaz Driver", que se encarga de comunicar los dispositivos biométricos (escaner y lector de código de barra) con la solución de caja y el segundo que tiene la misión de comunicar a la componente "Interfaz Driver" con la parte servidora de la solución, a la cual denominaremos "Middleware Cliente" y que tiene la capacidad de establecer comunicación con el servidor vía TCP/IP y SOAP. El detalle se muestra en la Figura 37.

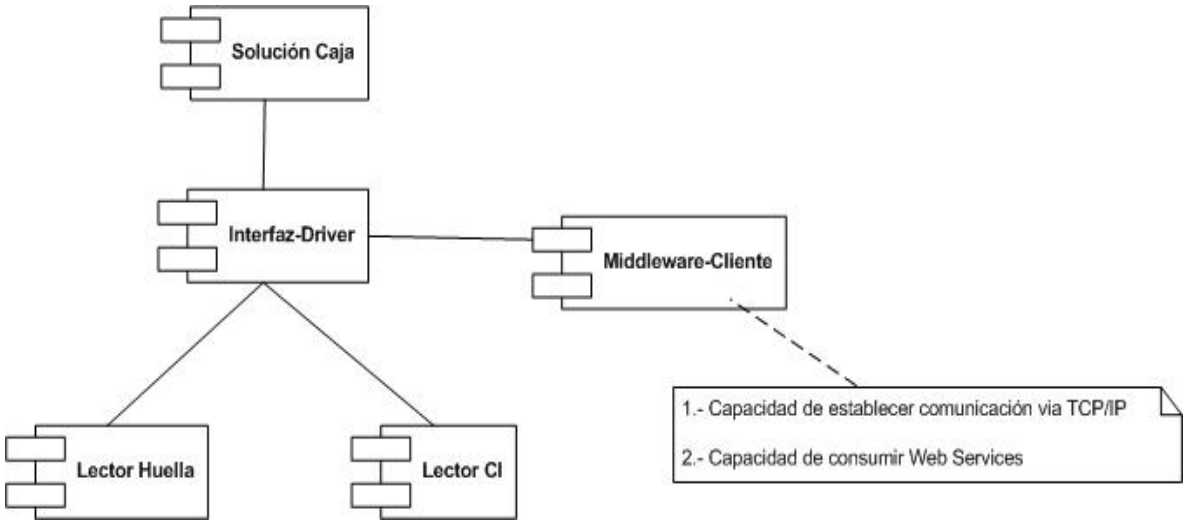

Figura 37 : Esquema de módulos en aplicación cliente

5.1.- **Identificación de piezas de software caja finesse** :

La solución de caja finesse se compondrá de 6 piezas de software, tres diseñadas e implementadas por el banco y tres desarrolladas por terceros que permitirán la operación con los dispositivos de captura.

Las componentes diseñadas por el banco son :

1) BechBioCaptor : Componente que presenta la interfaz a usuario e interfaces contra los dispositivos de captura (Interfaz-Driver).

2) BechClsBiometria : Componente de comunicación, que permite enviar los datos capturados al Host Banco, para su chequeo (Middleware-Cliente).

3) BechSerial-HDI : Componente que permite simular una entrada HDI para el dispositivo de lector de barras, es invocada por BechBioCaptor.

Las componentes de terceros son :

4) Drivers de lector Lumidign

5) Drivers emulador de puerto COM en puerto USB, para uso de lector de barra

6) API del lector Lumidign

1) BechBioCaptor :

Componente desarrollada en visual Basic 6, tipo proyecto Exe Active x. El nombre de clase del proyecto es "BechBioCaptor.clsenlace", tiene las siguientes funciones :

1.1) ChkDispositivo (arreglo_texto_in , arreglo_texto_out) :

Permite chequear que los dispositivos de lectura estén activos en el equipo. Para chequear el lector de barra se utilizará la componente BechSerial-HDI

1.2) Verificacion (arreglo_texto_in , arreglo_texto_out) :

Inicia la interfaz gráfica de la aplicación. Esta interfaz cuenta con la ventana de lectura de cédula y otra ventana de lectura de huella dactilar. Esta función utiliza BechSerial-HDI y BechClsBiometria. Los retornos válidos son :

"000" Verificación OK, DMA respondió OK
"001" Verificación Errónea, el DMA respondió rechazo
"002" Se leyó los datos pero no se recibe respuestas del DMA
"003" Se leyó la cédula pero no fue posible leer la huella del cliente y el usuario canceló el proceso
"004" Se leyó la cédula pero el usuario no leyó la huella y cancelo
"005" El usuario cancelo antes de leer la cédula
"006" Error en el DMA
"007" Error al crear objeto

1.3) Verificacion2 (arreglo_texto_in , arreglo_texto_out) :

Función clon de Verificación, que devuelve un string único en vez de un arreglo de string

1.4) TimeOut_LectorHuella :

Propiedad que cambia el valor de tiempo de timeout del lector de huella dactilar

2) Componente BechClsBiometria :

Componente desarrollada en Visual Basic 6, tipo proyecto DLL Active x. El nombre de clase del proyecto es "BechClasSTCP.TcpSend", tiene la siguiente función :

2.1) FxSendNec :

Envía la data al servidor DMA y espera la respuesta, la cual devuelve en el parámetro xRespuesta.

3) Componente BechSerial-HDI:

Este componente emula una interfaz de lector de código HDI, siendo que la configuración de los lectores es via puerto COM (puerto usb que emula puerto COM).

Componente desarrollada en Visual Basic 6, tipo proyecto Exe Active x. El nombre de clase del proyecto es "ATemuHDIfromSerial.clsEnlace", tiene las siguientes funciones :

3.1) Activar() : El programa abre el puerto COM, comienza la escucha

3.2) Desactivar() : El programa cierra el puerto COM y cesa la escucha

3.3) Cerrar_APP() : El programa cierra los puertos y termina su ejecución

3.4) Status : Devuelve un entero que representa el estado de la aplicación

3.5) PUERTO_COM : Estable o lee el puerto COM que se usará

5.2.- Identificación de archivos :

Archivo de log :

El sistema de caja biométrica tiene 2 archivos de log. Estos se activan o desactivan según el parámetro "LOG" del archivo Biometria.ini

HDI.log, corresponde al log de los programas BechSerial-HDI y BechBiocaptor

GWIso_*.GwIsoDat, corresponde al log de BechClsBiometria

Archivo de configuración :

El archivo de configuración se llama Biometria.ini, los 3 componentes leen información de configuración desde este archivo.

Descripción de la sección de configuración :

LU_TIMEOUT	Tiempo de espera del lector de huella
PORTLC	Puerto COM para uso de lector de cédula
LOG	Activación de log's de la aplicación : 0 desactivado, 1 activado
NEC_COINCIDENCIA	Texto devuelto por server DMA que indica la coincidencia
NFIQ	Valor mínimo de aprobación de calidad de la huella capturada
WAITXNEC	Tiempo de espera para el server DMA
PURGE_TIME	Tiempo en segundos en que el BechSerial-HDI no envía caracteres. Este tiempo corre después de la llamada a la función Activar

5.3.- **Servicio central de biometría** :

La validación biométrica es un valiosa herramienta de autenticación de personas, la incorporación de biometría ayuda a aumentar la seguridad de las transacciones bancarias con la consiguiente disminución en la cantidad de fraudes que se cometen

La implementación de biometría en Bancoestado induce la creación de un servicio central de biometría, tal servicio está soportado por un servidor web el cual a su vez envía requerimientos a otros dos servidores, al de Matching, donde esta instalado el producto NEC-DMA (Data Managment Array), que realiza la comparación de huellas y al de datos, donde se almacena el log biométrico producto de cada comparación.

El administrador de este servicio debe cumplir, al menos, las funciones que se describen a continuación :

1.- Administración de perfiles de usuarios de la aplicación de consulta a las transacciones en la aplicación DMA provista por NEC.

2.- Resolución de requerimientos sobre el Log biométrico, como por ejemplo, búsqueda de txn biométricas por periodo, Rut, etc. y obtención de huellas registradas en la autenticación.

3.- Asegurar la consistencia en la parametrización del DMA con su configuración en producción. Debe administrar parámetros tales como nombre base datos, nombre servidores, score de corte, etc.

4.- Efectuar el setup de la aplicación DMA.

5.- Validar que los componentes de la biometría central, tales como servidores de presentación, matching y datos, estén siempre disponibles.

6.- Responsable del sizing del sistema DMA, detectando permanentemente las nuevas necesidades, en función de las capacidades instaladas.

7.- Validar permanentemente la performance de la instalación y los posibles impactos en esta, producto de modificaciones en los canales.

8.- Apoyar las actividades de paso entre los ambientes existentes: Desarrollo, Test y Producción, en la perspectiva de desarrollo de nuevos proyectos de Biometría o mantenciones de estos.

9.- Diseñar, evaluar e implementar, los procesos de tunning del matching de la solución Biométrica central. Se debe definir política de riesgo v/s permisividad en el uso de la biometría.

10.- Apoyar la gestión de problemas a las áreas de producción y mesa de ayuda.

11.- Identificar aspectos de mejora desde el punto de vista de la performance.

12.- Asegurar la continuidad operacional del servicio de biometría central.

13.- Gestionar la necesidad de nuevos releases del DMA.

Este es proyecto es pionero en el banco en cuánto a la incorporación de Biometría, se espera que a futuro otras aplicaciones comiencen a utilizar la plataforma implementada efectuando los cambios que permitan soportar sus propias transacciones, en ese contexto, cobra relevancia la creación del servicio central de biometría y su necesaria administración.

6.- **Pruebas y puesta en producción** :

Las pruebas se harán a partir de instalaciones piloto en caja finesse y en caja vecina, dichas pruebas deben cubrir a todos los casos de uso definidos :

Caso 1 : Validación biométrica para pago a beneficiario que puede ser validado.

Caso 2 : VB para pago a apoderado que puede ser validado.

Caso 3 : VB para pago a beneficiario con mala calidad de huella.

Caso 4 : VB cuando no coinciden las huellas.

Complementario a las pruebas inducidas por los casos de uso, se agregan algunas otras pruebas a de elementos no funcionales que corresponden al contexto en que se explotará el sistema, entre estas pruebas tenemos :

- Eficacia y uso del Log biométrico
- Tunning de calce

Para conseguir la aceptación final de la plataforma se elabora un protocolo de aceptación en donde indicaremos las pruebas que se harán, la forma de implementarlas y cómo evaluarlas.

Se aprovechará este protocolo para adjuntar las evidencias obtenidas al efectuar cada una de las pruebas.

6.1.- **Protocolo de aceptación** :

Como una manera de validar el buen funcionamiento de la plataforma de validación biométrica se definen un conjunto de casos de prueba que deben ser hechas al sistema para verificar objetivamente que se cumplen todos los requerimientos que fueron solicitados, tanto a nivel funcional (que se puedan realizar los casos de uso previstos), como características no funcionales (por ejemplo, performance, capacidad, escalabilidad, robustez, etc.).

Los casos de prueba que componen el protocolo son los siguientes :

6.1.1.- **Casos de prueba funcionales** :

Prueba 1 :
Efectividad y funcionamiento de la validación biométrica en beneficiarios o apoderados que pueden ser validados.

Implementación :
Instalación de plataforma y de periféricos en al menos 2 cajas de sucursal piloto y en una caja vecina cercana a la sucursal.

Evaluación :
Cajeros y usuarios operativos verifican el funcionamiento del sistema, transacciones son registradas por log biométrico e informadas por el DMA.

Evidencias :
El Piloto fue realizado el día 15 de Diciembre de 2009 en la sucursal Colina, se verificó correctitud en los procesos de validación y a partir de los datos obtenidos se elaboró la siguiente estadística.

1.- **Volumen** :

Total mediciones biométricas :

Tipo de prueba	Cantidad
Transacciones reales	301
Pruebas	40
Total general	**341**

De éstas, **225** fueron transacciones efectivas realizadas por diferentes beneficiarios el día 15.

2.- **Eficacia** :

Del total de mediciones que no fueron pruebas :

Calce	Casos	%
Coincidencias	209	93%
No Coincidencias	16	7%
Total general	**225**	**100%**

3.- **Rechazos :**

Del total de mediciones que no fueron pruebas :

225 Beneficiarios atendidos
181 Beneficiarios pudieron ser validados biométricamente en el primer intento.
25 Beneficiarios pudieron ser validados biométricamente en el segundo intento.
3 Beneficiarios pudieron ser validados biométricamente en el tercer intento.
---
209 Total validados

8 Beneficiarios no pudieron ser validados biométricamente tras 1 intento.
5 Beneficiarios no pudieron ser validados biométricamente tras 2 intentos.
3 Beneficiarios no pudieron ser validados biométricamente tras 3 intentos.
---
16 Total rechazados

Tabla validados :

Intentos	%
Primer intento	80%
Segundo intento	11%
Tercer intento	1%
Total general	**93%**

Tabla rechazados :

Intentos	%
Tras 1 intento	4%
Tras 2 intentos	2%
Tras 3 intentos	1%
Total general	**7%**

Prueba 2 :
Rechazo en la validación biométrica.

Implementación :
Instalación de plataforma y de periféricos en al menos 2 cajas de sucursal piloto y en una caja vecina cercana a la sucursal.

Evaluación :
Cajeros y usuarios operativos verifican el funcionamiento del sistema, transacciones son registradas por log biométrico e informadas por el DMA.

Para este caso se debe tener en consideración que un rechazo en la validación biométrica corresponde a la identificación de un potencial fraude, por lo que se requiere de una definición de la Gerencia de Operaciones de Sucursales respecto a como operar frente a estos casos. La aplicación no solicitará clave supervisor y podrá el cajero operar inmediatamente bajo la modalidad "Sin Biometría".

Evidencias :
Las evidencias de estas pruebas están contenidas en el cuadro estadístico de la prueba anterior, en complemento se muestra un extracto de los datos generados a partir de las pruebas efectuadas.

JOBID	CUT_Banco	Fecha	Hora	Canal	Work station	RUT	Terminal	Oficina	Cod Transaccion	Score	Resultado
713	4,41897E+28	15-12-2009	09:32:01.463	0	5757	4418966-6	5757	330	8194	539	Coincidencia
714	4,17169E+28	15-12-2009	09:41:20.817	0	5757	4171692-4	5757	330	8194	0	No
715	1,40939E+29	15-12-2009	09:43:41.337	0	5757	14093888-2	5757	330	8194	1022	Coincidencia
718	6,34998E+28	15-12-2009	09:45:51.743	0	5757	6349977-3	5757	330	8194	1123	Coincidencia
719	1,30907E+29	15-12-2009	09:47:01.967	0	5757	13090657-5	5757	330	8194	1102	Coincidencia
720	4,86754E+28	15-12-2009	09:49:32.687	0	5757	4867540-9	5757	330	8194	0	No
723	1,19561E+29	15-12-2009	09:52:19.363	0	5757	11956111-6	5757	330	8194	4359	Coincidencia
724	1,28276E+29	15-12-2009	09:53:21.690	0	5757	12827593-2	5757	330	8194	686	Coincidencia
726	1,28276E+29	15-12-2009	09:54:35.570	0	5757	12827593-2	5757	330	8194	876	Coincidencia
727	1,66666E+29	15-12-2009	09:57:13.227	0	5757	16666649-K	5757	330	8194	3162	Coincidencia
728	1,66666E+29	15-12-2009	09:57:32.370	0	5757	16666649-K	5757	330	8194	1503	Coincidencia
729	7,83138E+28	15-12-2009	10:00:32.277	0	5757	7831381-1	5757	330	8194	1897	Coincidencia
730	7,83138E+28	15-12-2009	10:00:59.717	0	5757	7831381-1	5757	330	8194	868	Coincidencia
731	4,81857E+28	15-12-2009	10:02:28.827	0	5757	4818567-3	5757	330	8194	1271	Coincidencia
732	4,75029E+28	15-12-2009	10:05:45.830	0	5757	4750294-2	5757	330	8194	0	No
733	4,75029E+28	15-12-2009	10:06:34.347	0	5757	4750294-2	5757	330	8194	0	No
734	4,75029E+28	15-12-2009	10:06:58.097	0	5757	4750294-2	5757	330	8194	0	No
735	8,95206E+28	15-12-2009	10:08:32.163	0	5757	8952055-K	5757	330	8194	3453	Coincidencia
736	3,52973E+28	15-12-2009	10:10:40.227	0	5757	3529732-4	5757	330	8194	0	No
737	3,52973E+28	15-12-2009	10:10:59.697	0	5757	3529732-4	5757	330	8194	0	No
738	3,52973E+28	15-12-2009	10:11:16.260	0	5757	3529732-4	5757	330	8194	0	No
739	1,85227E+29	15-12-2009	10:11:38.883	0	4542	18522657-3	4542	330	8194	2211	Coincidencia
740	3,92974E+28	15-12-2009	10:13:16.340	0	4542	3929738-8	4542	330	8194	0	No
741	1,41255E+29	15-12-2009	10:14:30.683	0	5757	14125514-2	5757	330	8194	7299	Coincidencia
742	1,60415E+29	15-12-2009	10:15:10.450	0	4542	16041535-5	4542	330	8194	8303	Coincidencia

Prueba 3 :

Pago de beneficios a clientes que no puedan ser validados biométricamente (cédula de identidad antigua o huella ilegible).

Implementación y Evaluación :

La aplicación debe permitir efectuar el pago al beneficiario o apoderado sin efectuar validación biométrica.

Evidencias :

A partir de las pruebas efectuadas no fue posible obtener una muestra significativa de estos casos que permitiese generar alguna estadística respecto del porcentaje de clientes que no pueden ser validados, no obstante se pudo verificar que los pagos efectuados sin validación biométrica quedan registrados en el archivo de transacciones de caja mas conocido como 'Journal'.

Prueba 4 :

Evaluar usabilidad de los dispositivos, dificultad en el manejo y en la disposición de éstos en los puestos de trabajo.

Implementación :

Se requiere generar manuales simples de instalación. Evaluar entendimiento del personal de la sucursal piloto o caja vecina piloto.

Evaluación :
Mediante inspección visual de los encargados de operaciones de sucursales y cajas vecinas se debe chequear la disposición de los equipos en los puestos de trabajo, esto implica definir estándares para cada canal.

Evidencias :
Sin evidencia

Prueba 5 :
Percepción del servicio biométrico en clientes y usuarios internos.

Implementación y evaluación :
Definir encuestas sencillas para abordar a clientes que hayan sido atendidos con la biometría. También se requiere una encuesta con foco en el usuario (cajero)

Evidencias :
A partir de los pilotos no es posible acumular datos que sirvan para confeccionar estadísticas, se redactaron dos encuestas que serán aplicadas una vez que el sistema esté en producción, en su parte medular las encuestas consultan lo siguiente :

i) Para los cajeros :

	Muy Satisfecho	Satisfecho	Insatisfecho	Muy Insatisfecho
Calidad del sistema				
Facilidad de uso				
Calidad de documentación				
Rapidez en el uso de los dispositivos				
Confiabilidad en el sistema				

ii) Para los clientes :

	Muy Satisfecho	Satisfecho	Insatisfecho	Muy Insatisfecho
Calidad de la atención				
Confianza en el sistema				
Rapidez en la atención				

6.1.2.- **Casos de prueba no funcionales** :

Prueba 6 :
Generar Log biométrico.

Implementación y Evaluación :
Tomar muestra de pagos realizados en la sucursal y validar que estos se encuentren registrados en el Log biométrico.

Evidencias :
Se muestran dos informes obtenidos, el log genérico y el informe de actividades por fecha en el que puede observarse el resultado de las transacciones efectuadas.

Log Biométrico Banco Estado

Fecha Desde : 13/01/2010 11:34:00

Fecha Hasta : 15/01/2010 11:35:00

CUT	ID de Resultado (JobId)	Fecha Hora	Rut	Oficina	Terminal	Canal	Txn	Apellido Paterno	Nº Serie CI	Cod País
5,01142E+22	1249	14/01/2010 17:57	15662599	1	6	24	8194	GONZÁLEZ	A013651981	CHL
5,01142E+22	1252	14/01/2010 18:04	15662599	1	6	24	8194	GONZÁLEZ	A013651981	CHL
5,01142E+22	1253	14/01/2010 18:12	15662599	1	6	24	8194	GONZÁLEZ	A013651981	CHL
6,01142E+22	1250	14/01/2010 18:03	15662599	1	6	24	8194	GONZÁLEZ	A013651981	CHL
6,01142E+22	1251	14/01/2010 18:04	15662599	1	6	24	8194	GONZÁLEZ	A013651981	CHL

Actividades por Fecha

Fecha Desde : 13/01/2010 11:33:00

Fecha Hasta : 15/01/2010 11:34:00

CUT	ID Estación de Trabajo	ID de Resultado	CANAL	FECHA INICIO	RESULTADO	SCORE	TIEMPO INSUMIDO (ms)
5,01142E+22	5	1249	24	14/01/2010 17:57	Coincidencia	2313	1170
5,01142E+22	5	1252	24	14/01/2010 18:04	No Coincidencia	476	563
5,01142E+22	5	1253	24	14/01/2010 18:12	No Coincidencia	421	390
6,01142E+22	6	1250	24	14/01/2010 18:03	Coincidencia	895	1170
6,01142E+22	6	1251	24	14/01/2010 18:04	Coincidencia	1368	690

Prueba 7 :
Tunning de matching

Implementación y Evaluación :
A partir del resultado de validaciones biométricas OK y no OK, verificar si se requiere ajustar el umbral de validación biométrica definida internamente para el canal.

Evidencias :

Actividades por Fecha

Fecha Desde : 04/01/2010 14:31:00

Fecha Hasta : 11/02/2010 14:31:00

CUT	ID Estación de Trabajo	ID de Resultado	CANAL	FECHA INICIO	RESULTADO	SCORE	TIEMPO INSUMIDO (ms)
7,51074E+28	4542	2793	0	28/01/2010 10:32	Coincidencia	2452	300
6,50868E+28	4542	2795	0	28/01/2010 10:34	No Coincidencia	388	173
6,50868E+28	4542	2796	0	28/01/2010 10:34	**Coincidencia**	**519**	423
9,95923E+28	4542	2799	0	28/01/2010 10:36	**No Coincidencia**	**497**	686

Dado que los universos de prueba aún son pequeños se opta por no modificar el score y mantenerlo en 500. Una vez que se disponga de un mayor volumen de datos se podrán construir curvas de tasas de error (no calce) que permitan definir un score más representativo.

En relación a los criterios de aceptación definidos en el punto 3.5.- se pudo verificar que el sistema no presenta fallas de ninguno de los 3 tipos definidos.

6.2.- **Puesta en producción** :

Al cierre del presente trabajo, la plataforma computacional aún no era puesta en producción.

Existe una gran cantidad de componentes que deben estar en producción para asegurar el correcto funcionamiento de la plataforma. Los componentes productivos serán descritos según el diagrama de arquitectura descrito en el capítulo 4, esto es, según la funcionalidad que soportan y si residen en el cliente o en el servidor :

6.2.1.- **Componentes Servidor** :

Las aplicaciones que residen en la parte servidora son las siguientes :

6.2.1.1.- **Web Server** : Es el servidor que contiene los aplicativos Images Processor e Image Proccesor Service Manager

- **Nombre sugerido** : S3K-BIOAPP01

- **Hardware** : Las especificaciones técnicas son las siguientes :

Descripción	Característica
Chasis en Rack	Rack-Mountable form factor
Procesador	4 Intel Xeon ™ MP
Crecimiento en procesadores	No
Velocidad del Procesadores	2.7 GHz
RAM Base y tipo	4 GB
Memoria Cache y nivel	Cache 2 MB L3 y 512 Kb L2
Arquitectura	Cliente / Servidor
Controlador de disco	SCSI-3 Ultra3 Wide
Capacidad en Disco en chasis	2 x 36 GB, de 15 K rpm

Software :

Sistema operativo : Windows 2003 Server SP2
Software base : Image Processor Service Manager
Image Processor
JDK 5.0 (Java development kit)
Middleware Servidor
Job Controler

6.2.1.2.- **DMA** : Es el servidor que contiene el aplicativo DMA Web.

- **Nombre sugerido** : S3K-BIODMA01

- **Hardware** : Las especificaciones técnicas son las siguientes :

Descripción	Característica
Chasis en Rack	Rack-Mountable form factor
Procesador	4 Intel Xeon ™ MP
Crecimiento en procesadores	No
Velocidad del Procesadores	2.7 GHz
RAM Base y tipo	4 GB
Memoria Cache y nivel	Cache 2 MB L3 y 512 Kb L2
Arquitectura	Cliente / Servidor
Controlador de disco	SCSI-3 Ultra3 Wide
Capacidad en Disco en chasis	2 x 36 GB, de 15 K rpm

Software :

Sistema operativo : Windows 2003 Server SP
Software base : DMA Web
DMA IOCS

6.2.1.3.- **Log biométrico** : Es el servidor que contiene la base de datos utilizada por los productos involucrados en el proyecto biometría.

- **Nombre sugerido** : S3K-BIODAT01

- **Hardware** : Las especificaciones técnicas son las siguientes :

Descripción	Característica
Chasis en Rack	Rack-Mountable form factor
Procesador	4 Intel Xeon ™ MP
Crecimiento en procesadores	No
Velocidad del Procesadores	2.7 GHz
RAM Base y tipo	4 GB
Memoria Cache y nivel	Cache 2 MB L3 y 512 Kb L2
Arquitectura	Cliente / Servidor
Controlador de disco	SCSI-3 Ultra3 Wide
Capacidad en Disco en chasis	2 x 36 GB, de 15 K rpm

Software :

Sistema operativo : Windows 2003 Server SP
Software base : SQL Server 2005
Log biométrico

6.2.2.- **Especificación de instalación** :

El Orden de Instalación deseado es :

1.- Instalación BD

a. DMA_SECURITY
b. DMA_DATABASE
c. DMA_DATABASE_STORE

2.- Instalar DMA Web

3.- Instalar AFISIOBankWS (DMA IOCS)

4.- Instalar DMAImagesProcessor

5.- Instalar DMAImagesProcessorServiceManager

6.- Middleware Servidor

7.- Job Controler

6.2.3.- **Componentes Cliente** :

Las aplicaciones que residen en la parte cliente y que deben ser instaladas son :

6.2.3.1.- **Caja finesse y caja vecina** :

Hardware :

- Driver lector de huella
- Driver lector de CI

Software :

- Interfaz Driver
- Middleware Cliente

La aplicación de caja finesse es versionada, esto significa que cada actualización de software debe ser instalada en cada caja en forma directa, esto implica gran cantidad de tiempo ya que se debe recorrer el país entero para instalas los componentes en cada una de las sucursales.

7.- **Conclusiones** :

Uno de los objetivos de Bancoestado es apoyar la gestión del Estado de Chile prestando servicios a diversos organismos públicos. Con la culminación de este trabajo se asegura el correcto destino del pago de beneficios, de todo tipo, que el Estado entrega a los pensionados a través del IPS.

No puedo desligar las conclusiones finales de los objetivos planteados al comienzo de este trabajo. El objetivo principal, diseñar e implementar una plataforma computacional que permita aplicar seguridad biométrica dactilar en el pago de beneficios del IPS, no sólo se cumplió satisfactoriamente sino que de paso cumplió con el objetivo no declarado de ser un proyecto pionero en cuánto a la inclusión de seguridad biométrica en la identificación de personas.

La validación biométrica contribuye a disminuir los fraudes a que están expuestos los sistemas bancarios, es por ello que, gracias a la experiencia adquirida en este proyecto, otras áreas del banco están estudiando la forma de aumentar la seguridad de sus sistemas vía la aplicación de seguridad biométrica.

Se pudo comprobar que el tiempo de atención de los beneficiarios en las cajas no disminuyó, incluso aumentó levemente ya que se agregó un paso más en la atención. Esto hace que uno de los objetivos originales no se haya cumplido, a cambio se ganó en confiabilidad por parte de los beneficiarios y en seguridad de gestión por parte de los cajeros.

Los diseños de Arquitectura, de interfaces de comunicación y de interfaces de usuarios fueron elementos claves en el éxito de esta memoria por lo que se concluye como objetivos intermedios cumplidos.

La parte inicial de este trabajo consistió en evaluar diferentes dispositivos lectores de huella y en analizar sistemas de comparación de imágenes digitales, el proyecto se hizo viable a partir de la tecnología de calce de imágenes disponible en el mercado nacional, sin ello, ni siquiera se hubiese pensado en implementar un proyecto de esta naturaleza.

El escaso volumen de datos impidió la generación de curvas de tasas de error que permitiesen obtener un score de aceptación más representativo, no obstante una de las primeras actividades de la administración del servicio central de biometría será la de generación de dichas curvas una vez que se disponga de un mayor volumen de datos

Si bien la metodología fue un marco de referencia, no se usó en todo su potencial principalmente por dos razones, primero porque el Banco estaba comenzando a introducir esta nueva metodología mientras el proyecto ya estaba en desarrollo y segundo por las particularidades del proyecto, con varios proveedores externos y uso de hardware y software ya construido, no obstante igual se siguieron las etapas definidas y se usaron varios de los artefactos propuestos.

La experiencia ganada y los conocimientos adquiridos son un valioso capital que queda en manos de los participantes de esta iniciativa. La plataforma implementada, proyecto de vanguardia en cuanto a seguridad biométrica, queda a disposición de Bancoestado.

Los pensionados del IPS son, en su mayoría, personas de edad muy avanzada, trabajar en un proyecto destinado a mejorar la atención hacia ellos constituyó una motivación especial y conseguir las metas propuestas ha sido objeto de una gran satisfacción personal.

8.- **Bibliografía** :

1.- Enciclopedia electrónica Wikipedia.

2.- Tecnología biométrica dactilar en el mercado financiero, presentación de Nec Chile.

3.- John D. Woodward Jr, Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York : McGraw Hill Osborne, 2003).

4.- Object-Oriented Software Engineering, Timothy C. Lethbridge and Robert Laganiere.

5.- Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

6.- Secugen Biometrics Solutions http://www.secugen.com/images/faq02.gif.

7.- International Biometric Group http://www.biometricgroup.com.

8.- Manfred Bromba, "Bioidentification : Frequently Asked Questions" http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensore

9.- **Anexos** :

9.1.- **Ambientes** :

Diagrama de servidores, desarrollo, test y producción

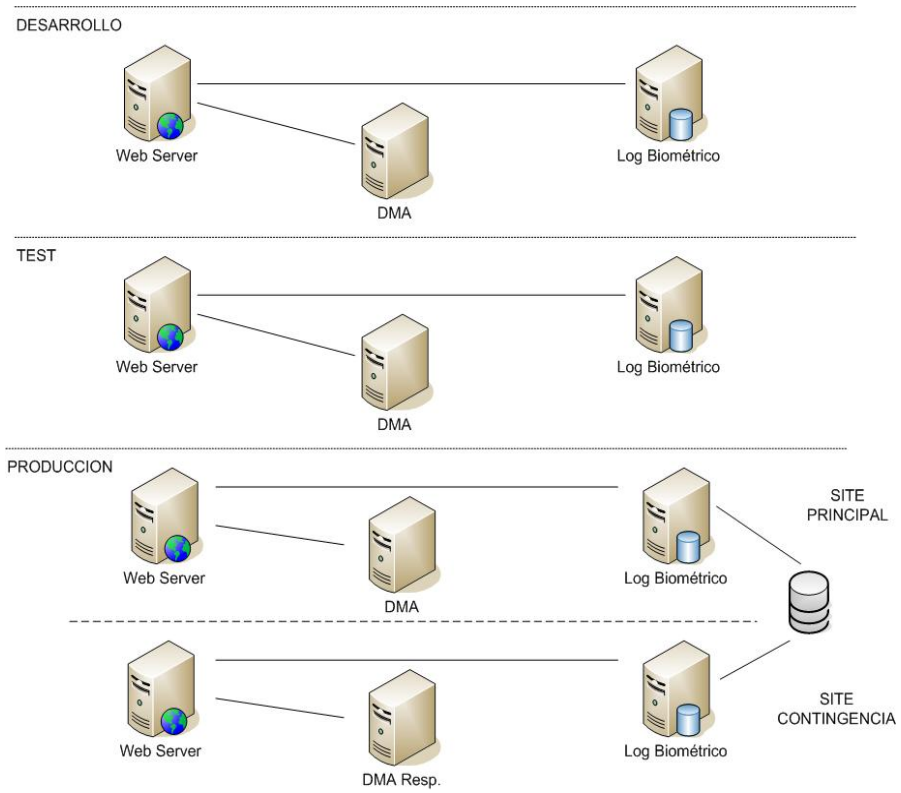

Figura 38 : Servidores necesarios para el proceso de validación biométrica

9.2.- **Requerimientos de hardware** :

i) Ambiente de Desarrollo, 3 servidores virtuales con las siguientes características :

Servidor Web :

1 Procesador
4 Gigas en memoria RAM
40 Gigas en disco

Servidor de Match :

2 Procesadores
4 Gigas en memoria RAM

40 Gigas en disco duro

Servidor de datos :

1 Procesador
4 Gigas en memoria RAM
40 Gigas en disco duro

ii) Ambiente de Test, 3 servidores virtuales con las siguientes características :

Servidor Web :

1 Procesador
4 Gigas en memoria RAM
40 Gigas en disco

Servidor de Match :

4 Procesadores
4 Gigas en memoria RAM
40 Gigas en disco duro

Servidor de datos :

1 Procesador
4 Gigas en memoria RAM
40 Gigas en disco duro

iii) Ambiente de Producción, 6 servidores físicos con las siguientes características:

Servidor Web (2) :

2 Procesador
4 Gigas en memoria RAM
70 Gigas en disco

Servidor de Match (2) :

4 Procesadores
4 Gigas en memoria RAM
70 Gigas en disco duro

Servidor de datos (2) :

4 Procesador
16 Gigas en memoria RAM
600 Gigas en disco duro
Tarjeta de fibra para discos Shark