FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

"ESTUDIO DE PRE FACTIBILIDAD PARA IMPLEMENTAR BIOMETRÍA MEDIANTE HUELLA DIGITAL EN LA RED DE CAJEROS AUTOMÁTICOS, BANCO DE CRÉDITO DEL PERÚ"

Tesis para optar por el Título Profesional de
Ingeniero de Sistemas de Información y Gestión

Presentado por:

César Augusto Monjaraz Mazzei

LIMA – PERÚ

2015

ÍNDICE

ÍNDICE DE FIGURAS Y GRÁFICOS

ÍNDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

La reducción de costos es lo que busca cualquier organización, viendo de mejorar sus procesos y su tecnología que a largo plazo trae ahorro y beneficios. Este proyecto considera el objetivo estratégico que como Área de Canales Alternativos se tiene que es el de migrar transacciones a canales no convencionales, así como el de seguridad y tecnología. La investigación está compuesta por cinco capítulos que describo a continuación.

En el primer capítulo planteo la problemática que da motivo a este estudio poniendo el contexto en la que se encuentran los canales de atención y de manera más particular el canal ATM. Es importante dar a conocer la proporción de transacciones que actualmente no podemos atender al no poder identificar a los "no clientes", y las vulnerabilidades y desventajas que tenemos como justificación. Estableceremos también el objetivo general que es el de dar a conocer una nueva forma de acceso implementando biometría en la red de cajeros automáticos, que es el norte para esta investigación.

En el segundo capítulo daremos a conocer mediante el marco teórico las principales definiciones sobre los cajeros automáticos, conociendo sus tipos y funciones. Definiremos a la biometría como centro de nuestro estudio y a las distintas tecnologías que hoy aplican en este campo. Mostraremos cómo es el proceso de autenticación biométrica por huella dactilar en comparación con la identificación actual. Mencionaremos también qué es el fraude y cuáles son los tipos que están presentes en nuestro territorio. Al final RENIEC nos facilitará toda la información referente al DNI electrónico que será clave para nuestra investigación y como esto ayudará con el nuevo proceso de autenticación en los ATMs. Finalmente daremos a conocer a la Gerencia de Canales Electrónicos como unidad a cargo de los cajeros automáticos.

Pasamos al tercer capítulo donde se describirá el método a seguir y la definición de las variables que participan. Mencionaremos un resumen de la teoría del método estadístico SARIMA y del coeficiente V de Aiken para darle mayor sustento científico a nuestra investigación. Es importante tener en cuenta el comportamiento transaccional para hacer estimaciones del negocio y poder proyectar las oportunidades que se vienen.

En el cuarto capítulo se mostrarán los resultados del análisis y como estos darán sustento para en un futuro implementar la biometría de forma masiva a toda la red de agencias y puntos neutros. Mostraremos la proyección transaccional a través del modelo SARIMA utilizando el paquete estadístico EViews, las ventajas de la biometría en el aspecto de seguridad, los intervalos de confianza por el coeficiente V de Aiken utilizando el software de ICaiken, también la posición del banco de forma competitiva al contar con más funcionalidades y finalmente los costos asociados en este estudio de pre factibilidad.

Los resultados mostrarán sólo el inicio de lo que será un cambio innovador en el comportamiento de nuestros usuarios y nuevas oportunidades para el área de Canales Alternativos y la División Comercial.

En el quinto capítulo está la discusión que se analizará desde el marco teórico y la concordancia con los resultados que se mostrarán, dando detalles sobre lo obtenido.

Finalmente en el sexto capítulo terminaremos este documento con las conclusiones y recomendaciones presentando la viabilidad del acceso mediante biometría de huella digital en los ATMs, la bibliografía requerida para avalar la investigación y los anexos con información adicional para su desarrollo.

ABSTRACT

Reducing costs is what all companies are looking for to improve its processes and technology, bringing long-term savings and benefits.

This project considers the strategic goal that as Alternative Channels Area have, as well as security and technology. The investigation consists in five chapters which I describe below.

In the first chapter we propose the issue that gives reason to this study, putting in context in which they are the attention channels and more particularly, the ATM channel. It is important to mention the proportion of transactions that currently can´t identify "non-customers", and vulnerabilities and disadvantages we have as justification. Also we establish the general objective and specific objectives that will be the north for this research.

In the second chapter we will present the framework with the main definitions of ATMs, learning their types and functions. We define biometrics as the center of our study and the different technologies that today apply in this field. We show how the process of biometric fingerprint authentication is compared with the current identification. Also mention what is fraud and what are the types that are present in our territory. At the end RENIEC provide us all the information concerning the electronic ID document that will be the key for our investigation and how this will help with the new authentication process at ATMs. Finally we will present to management electronic channels as a unit in charge of ATMs.

We will pass to the third chapter where the following method will be described and the definition of the variables involved. We mention a summary of the statistic method Sarima and the V Aiken Coefficient to give more scientific sustentation to our investigation. It is important to note transactional behavior to do business estimations and can project the coming opportunities.

In the fourth chapter the analysis results will be displayed and how these will give support in the future to implement biometrics in massive form to the entire network of agencies and neutral points. We will show the transactional projection, the advantages of biometrics in the security aspect, the validity of the criteria of expert judges and at the end the competitive position of the bank.

The results will show only the beginning of what will be an innovative change in the behavior of our users and new opportunities for the area of Alternative Channels and Commercial Division. In the fifth chapter is the discussion to be analyzed from the theoretical framework and concordance with the results to be display, giving details on the proceeds.

Finally in the sixth chapter this document presents the conclusions and recommendations of the access feasibility through fingerprint the biometric ATMs,

the bibliography to endorse the literature research and annexes with additional information for its development.

INTRODUCCIÓN

La accesibilidad a los servicios financieros en los países de América Latina ha cobrado especial importancia en la actualidad. Esto lo vienen trabajando tanto los gobiernos, empresas privadas y sobre todo las entidades financieras.

Los aspectos a considerar para que la accesibilidad sea la adecuada es básicamente la cobertura geográfica del territorio. No todas las zonas se encuentran homogenizadas debido a la ubicación.

En el Perú, y gracias a la actividad económica tan dinámica, la bancarización se ha incrementado en los últimos años. Acompaña a esto la descentralización en las provincias, donde se encuentra miles de potenciales clientes que aún no cuentan con acceso a servicios bancarios y/o financieros.

En medio de este proceso de bancarización las entidades financieras buscan tener mayor presencia en la economía, brindando mayor comodidad y rapidez en las transacciones que realizan sus clientes. Esto se logra a través de los canales alternativos de atención, que buscan llegar de manera más eficiente a los usuarios.

Los canales alternativos nacen con la idea de poder brindar atención 24 x 7 (los 7 días a la semana, 365 días al año) y llegar a lugares remotos. En un inicio el despliegue fue tener cobertura pero luego no solamente el Banco busca hacerlo un canal auto atendible o de auto servicio, sino que también sea uno de ventas donde el cliente pueda encontrar productos financieros a la medida de sus necesidades.

El documento presenta el estudio de pre factibilidad y los usos que se tendrían al realizar la identificación mediante biometría para acceder a los servicios en los cajeros automáticos que permitirá llegar de una manera más eficiente y efectiva a los usuarios.

La migración de transacciones es traducida en ahorro al reducir los costos operativos al realizar una transacción de ventanilla en el cajero automático. La puesta en marcha del nuevo DNIe (DNI electrónico) promovida por RENIEC nos favorece considerablemente.

Adicional a esto la nueva tecnología trae mejoras en la seguridad que ayudaran a prevenir las distintas modalidades de fraude que hay en el mercado local y a reducir las pérdidas que estos actos generan. En general tanto el Banco como sus usuarios se verán verdaderamente beneficiados con los frutos de este trabajo.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

El no estar a la vanguardia en el aspecto tecnológico puede privar de grandes beneficios a las empresas, en este caso a las entidades bancarias, que no pueden darse el lujo de perder usuarios o dejar de atenderlos. El Banco como parte de su política de prevención de lavado de activos no permite realizar algunas operaciones en caso el usuario no pueda identificarse y aquí es donde, por ejemplo, no podemos atender las transacciones de los “no clientes” en nuestros cajeros automáticos que solamente permiten el acceso al menú transaccional a los clientes mediante el uso de una tarjeta (crédito o débito).

Considerar que la atención de usuarios (clientes y no clientes) en los canales convencionales, como lo es la ventanilla a través del Promotor de Servicios, tiene un costo altísimo ya que se basa en un recurso humano. El eje estratégico del Área de Canales Alternativos es el de migrar las transacciones de estos canales convencionales a otros canales como los cajero automáticos, agente, plataforma virtual, Banco Celular, Banca por Internet, centro de contacto, SMS, etc.); por lo que está constantemente en la búsqueda de innovación para poder lograrlo.

Por la parte de seguridad se presentan distintas clases de delitos informáticos que intentan vulnerar los sistemas y procesos. Estos ataques se dan frecuentemente, por lo que hay que estar atentos a los mecanismos y modalidades de fraude. En la actualidad existen diversas formas de fraude como puede ser el robo de identidad por suplantación, el “cambiazo”, la clonación mediante la instalación de dispositivos (hardware) e incluso el intento de robo de data encriptada (hardware y software). Las bandas de delincuentes y cyber delincuentes tienen acceso a dispositivos modernos que manipulan para cometer actos ilícitos y que los usuarios no percibimos al utilizar un servicio de este tipo. El Banco y los usuarios actualmente tienen grandes pérdidas ocasionadas por los distintos tipos de fraudes.

Por último, considerar que los bancos brindan cada vez más funcionalidades nuevas para poder dar mejor atención a sus clientes. Es así que una entidad gana posicionamiento respecto a las otras cuando tiene un factor diferenciador y es el caso de otros bancos que pueden atender operaciones de “no clientes” en sus cajeros automáticos.

1.2 Formulación de la Pregunta de Investigación

1.2.1 Pregunta General

¿Será factible presentar una nueva forma de acceso al implementar biometría mediante huella dactilar en la red de cajeros automáticos de una entidad financiera de Lima Metropolitana?

1.2.2 Preguntas Específicas

¿Permitirá migrar transacciones al canal ATM al atender a los “no clientes”?

¿Permitirá presentar las vulnerabilidades del sistema de identificación actual contra las ventajas de la biometría?

¿Permitirá competir con otras entidades financieras que ya cuentan con cajeros automáticos que atienden operaciones de “no clientes”?

¿Permitirá presentar los costos que demandaría su implementación?

1.3 Justificación

En la actualidad los canales alternativos brindan más opciones a los clientes para poder realizar sus transacciones, adicional a las agencias bancarias tradicionales. El Banco atiende de manera mensual a más de seis millones de clientes, los cuales sumados a los no clientes realizan alrededor de 65.71 millones de transacciones, donde el 90% utiliza los canales alternativos como ATM, agente, Banca por Internet y Banca Celular. En lo que corresponde a cajeros automáticos tenemos alrededor de 14 millones de transacciones mensuales, datos obtenidos del Área de Planeamiento de Canales.

El 50% de las transacciones que se realizan en ventanilla las realizan no clientes y el 76% de estas transacciones son pagos de servicios, depósitos y pagos banco. Los costos de atención en ventanilla son los más altos que existen en la organización, costando aproximadamente s/. 3.8 cada una, por ende la premura de poder reducir estos derivándolos al canal ATM. También consideremos que el Banco busca brindar mayor rapidez y comodidad a sus usuarios mediante los canales de atención.

Los mecanismos de fraude como son la clonación, la suplantación, el “cambiazo”, entre otros; están al acecho en mayor proporción en nuestro país. Utilizar tecnología de última generación mediante la biometría de huella dactilar hará tener una mejor posición frente a este.

Nuestros canales de autoservicios y ventas están en la capacidad de ser explotados de forma más eficiente, explorando alternativas innovadoras para así ofrecer a nuestros usuarios mayores y mejores servicios, y que a su vez el banco se beneficie.

1.4 Delimitación y Alcance

1.4.1 Delimitación temporal y espacial

El estudio se comprende con información hasta el mes de julio-agosto del 2015 y se realizará entre los meses de setiembre a noviembre del 2015.

El estudio se realiza en base a la red de cajeros de la entidad financiera materia de estudio dentro del territorio nacional.

1.4.2 Alcance

La presente investigación solamente tomará en cuenta el estudio y análisis para implementar el lector biométrico en la red de cajeros del Banco basándose en la información y elementos que aporten criterios para elaborar juicios que den valor al rol de los canales electrónicos.

1.5 Limitaciones

Limitaciones en la información respecto al Área de Seguridad y Prevención de Fraudes para tener un mapa claro de la cantidad de reclamos por denuncias de este tipo de actos delictivos y las cifras de pérdida en los últimos años / meses.
Limitaciones en la información respecto al detalle por operación y tipos de operación del Área de Planteamiento de Canales de la División Comercial, solamente contamos con cifras totales que de igual manera son de mucha ayuda para este estudio.
Limitaciones de las especificaciones técnicas del proveedor Diebold sobre la funcionalidad de entrega de duplicado de tarjeta en ATMs multifunción.

1.6 Objetivos de la Investigación

1.6.1 Objetivo General

Desarrollar un estudio de pre factibilidad para presentar una nueva forma de acceso a los servicios de cajeros automáticos implementando lectura biométrica por huella dactilar, y sus usos.

1.6.2 Objetivos específicos

- Proyectar las transacciones del canal ATM al poder atender a los “no clientes”

- Presentar las ventajas de la biometría ante las vulnerabilidades de la seguridad del proceso de identificación actual

- Presentar que con la biometría el Banco estaría mejor posicionado respecto a otras entidades financieras que ya cuentan con ATMs que atienden operaciones de “no clientes”

- Presentar los costos que demandaría su implementación

1.7 Hipótesis

1.7.1 Hipótesis General

Sí es posible desarrollar un estudio de prefactibilidad para presentar una nueva forma de acceso a los servicios de cajeros automáticos implementando lectura biométrica por huella dactilar, y sus usos.

1.7.2 Hipótesis Específicas

- Se apreciará un incremento en la proyección del nivel transaccional al canal ATM respecto a los años anteriores
- Se reducirán las vulnerabilidades de seguridad del proceso de identificación actual
- La entidad financiera se posiciona en primer lugar respecto a las funcionalidades del canal ATM
- Los costos que demandaran la implementación de la biometría no serán significativos

CAPÍTULO II. ANTECEDENTES Y MARCO TEÓRICO

2.1 Antecedentes

La entidad financiera del presente estudio es uno de los más grandes del pais la cual tiene una amplia red de agencias y de canales de atención. A base del gran crecimiento empezó su expansión a través de su red de agencias, nuevos productos financieros y la instalación de cajeros automáticos, entre otros. Actualmente el banco cuenta con presencia en casi todas las plazas a nivel nacional y con una extensa red de cajeros automáticos.

En el ámbito de canales alternativos existen también otros bancos con redes bastante amplias. Todas estas redes, y en particular la de cajeros automáticos, sufren ataques constantemente por lo que tienen que implementar nuevos procesos y sistemas de seguridad para resguardar a sus clientes y su información. Cuando una empresa desea implementar una nueva tecnologia se deben considerar los requisitos básicos, asi como los costos e impacto en el negocio.

En el pais no se han tomado al momento medidas de seguridad que permitan reducir este tipo de ataques. Los cajeros automáticos del parque nacional en promedio siguen teniendo como minimo máquinas de hace 4 años y a pesar que existen dispositivos que re potencian al equipo y brindan seguridad al cliente, se tiene que seguir innovando con nuevas medidas.

En el plano internacional Navarrete (2012), del diario Biobio de Chile, a través de su artículo “Banco japonés implementará cajeros automáticos biométricos que escaneará la mano del cliente” indicó que en Japón se lanzó en el año 2012 el escaneo por palma de mano en los cajeros automáticos, la primera forma de biometria en una red existente de gran magnitud, de esta forma fueron los pioneros al atender clientes sin tarjetas para realizar sus operaciones. El Ogaki Kyoritsu Bank es el nombre de la entidad que lo realizó apuntando a la reducción de la clonación de tarjetas. El cliente solamente tiene que identificarse en una agencia para hacer el registro de sus datos biométricos y numéricos para la autenticación, esto ayudaria mucho en casos en los que el cliente olvide o no cuente con su tarjeta o en desastres donde prácticamente no podrias tener acceso a los servicios bancarios.

A nivel de América Latina López (2014), del diario No sólo Economia, a través de su artículo “Banco Santander Brasil implanta la biometria” comentó que el Banco Santander ya se adelantó implementando la biometria de huella dactilar en la red de oficinas y cajeros automáticos; para esto se han valido de la empresa Vector ITC Group. Se inició en 200 oficinas solamente y al 2014 se tenia en más de 3783 cajeros automáticos. El proceso sigue siendo el mismo para los casos de consultas y movimientos pero para realizar una operación monetaria se requiere el uso de huella dactilar para su confirmación. En palabras del Director del área Software Products & Outsourcing de Vector ITC Group, Luis Asensio, *“una vez que los clientes se habitúen al uso de la biometría y finalice el roll out masivo habilitaremos*

en el ATM la opción de dispensaciones rápida sin tarjeta/pin, en cantidades no superiores a 500 euros reales".

Vector utiliza la biometría más estándar que es mediante *finger print* o impresión dactilar ya que está es sencilla de implementar y es la que se ha adoptado en su mayoría a nivel mundial para distintas entidades privadas y del estado. En general esta solución aporta seguridad, robustez y eficiencia (Vector-ITC Group, 2014).

Ventas de Seguridad (2012) indicó que "Lumidigm está trabajando con Itautec, proveedor de servicios informáticos brasileño, para la instalación de las primeras 12.000 unidades de la red de 33.000 ATM. Los lectores no solo le proporcionan a los clientes el acceso seguro a sus cuentas, sino que además garantizarán que cada persona tenga solamente una identidad."

En el panorama nacional el diario Gestión (2012) a través del artículo "Interbank comienza pruebas de reconocimiento facial en cajeros automáticos "mencionó que el Interbank inició lo que serían las primeras pruebas de biometría por reconocimiento facial en su red de cajeros automáticos Globalnet. En alianza con la empresa española F7 Corporation, la idea era fortalecer las medidas de seguridad. El sistema de identificación funciona por patrones que son comparados mediante algoritmos que utilizan la distancia de los ojos, labios, nariz, entre otros. Al día de hoy no se han tenido más novedades de manera pública al respecto pero se entiende que en laboratorio deben contar con avances muy interesantes que pronto estarán disponibles para todos los clientes.

2.2 Marco Teórico

2.2.1 Cajeros Automáticos

Según IESNA, 1997(citado por Klecius, 2007, p.14) el cajero automático o ATM (automated teller machine) es un terminal financiero de autoservicio que permite a los clientes de las entidades financieras acceder a los servicios bancarios tales como retiro de efectivo, consulta de saldos y movimientos, transferencias, etc.; sin la necesidad de ser operado por un ser humano.
En otra definición Handson Banking (2015) indicó que el cajero automático es "una computadora especializada usada por los clientes bancarios para manejar su dinero. Por ejemplo, casi todos los cajeros automáticos le permiten retirar dinero, y muchos de ellos también le permiten hacer depósitos."
Hoy en día hay cajeros que permiten realizar ya no solamente retiro de efectivo si no también depósitos entre otras funcionalidades.

2.2.1.1 Tipos

Los cajeros que existen en los bancos y cajas en el Perú son los de retiro y los multifunción, llamados así porque adicional a los retiros permiten realizar depósitos.

2.2.1.2 Partes

Diebold es el principal proveedor local de cajeros automáticos por lo que se presenta información de esta empresa. De cara al cliente un cajero de retiro en el mercado local está compuesto por la pantalla o monitor, botones funcionales, teclado numérico, impresora, parlante, bandeja de dispensación, jack o entrada hembra para audio y lector de tarjeta (véase Figura 1).

Por la funcionalidad de los dispositivos estos se dividen en dispositivos de entrada y de salida. Se van a nombrar los dispositivos de entrada que están expuestos en la parte exterior, estos son (Diebold, s.f.):

- Lector de tarjeta: Dispositivo que captura la información de la banda magnética o chip de la tarjeta (smart card) para poder identificar al usuario
- Teclado numérico: Dispositivo que permite recibir información numérica para ingresar datos como DNI, cantidad o contraseña
- Botones funcionales: Son botones que permiten señalar la transacción que el usuario quiere realizar, a qué cuenta, tipo de moneda, etc.
- Bandeja de depósito: Dispositivo que recibe dinero en efectivo para realizar una operación de depósito

Los dispositivos de salida son:

- Parlante: Dispositivo que emite ruido en respuesta a la acción del usuario
- Jack: Dispositivo para dar guía por voz a videntes (opción no habilitada actualmente)
- Pantalla: Monitor a colores que muestra los pasos a realizar a los usuarios y permite una interacción mediante una interfaz gráfica
- Impresora: Dispositivo que imprime los recibos por la transacción realizada - Bandeja de Dispensación: Dispositivo conectado al dispensador que entrega en una bandeja el dinero en efectivo

El cajero multifunción o de depósito está compuesto por las mismas parte pero adicionalmente cuenta con la bandeja de depósito (véase Figura 2).

A lo interno el cajero también tiene distintas partes como lo son el CPU (tal como una computadora convencional), bóveda, dispensador, bandeja de rechazo e impresora.

- Bóveda: Es la caja fuerte totalmente armada de acero tiene en su interior las loncheras que son pequeñas cajas donde se almacenan los billetes (véase Figura 3)
- Dispensador: Dispositivo que procesa el billete desde las loncheras hasta la bandeja de dispensación (véase Figura 4)
- Lector de tarjeta: Dispositivo que lee las tarjetas de banda magnética y las tarjetas inteligentes (véase Figura 5)

- Impresora: Maquina termo magnética que imprime los recibos por la transacción que se realiza. Cuenta aparte con un rollo de papel para poder imprimir
- Lonchera: Es un cassette donde van los billetes y se encuentran agrupaos en una bandeja dentro de la bóveda. El dispensador saca desde aquí los billetes por cada transacción (véase Figura 6)

Bandeja de rechazo: Es un pequeño cassette pero no al igual que las loncheras donde van los billetes que no pueden ser procesados por algún motivo como atraco en la dispensación, mala calidad del billete o que se encuentran muy doblados.

Tenemos entonces que hay dispositivos de entrada y de salida, algunos de los cuales son conocidos por encontrarse a la vista o ser obvios y otros que se encuentran al interior que la mayoría de usuarios desconoce de su existencia o su función.

Al interno el ATM está conectado a una computadora que es la que establece la comunicación entre el sistema operativo Windows y KAL (software principal), así como para el manejo de los distintos dispositivos externos. Las máquinas del parque actual cuentan con las siguientes especificaciones técnicas:

- Procesador Pentium D 64 Bits 1.6 Ghz.
- Memoria RAM 1Gb.
- Disco Duro de 120 Gb.
- Sistema Operativo Windows XP SP3
- Puerto USB 2.0
- DVD ROM
- Pantalla 14”
- Mini teclado estándar

Las distintas partes y componentes mencionadas son las que son necesarias para que un cajero automático funcione.

2.2.1.3 Operaciones en los Cajeros Automáticos

Las entidades financiera locales indicaron que en los cajeros automáticos se pueden hacer cada vez mayor cantidad de operaciones donde la principal es el retiro de efectivo. Hay una fuerte competencia por presentar mayores funcionalidades a los clientes con el fin de poder captarlos. Tenemos entre las últimas habilitaciones al “Efectivo móvil”.
En general en todos los bancos locales se tienen las mismas operaciones y solamente algunos cuentan con el factor diferenciador, aunque no lo es todo para determinar el gusto del cliente.

Se muestran a continuación las operaciones más comunes realizadas en los cajeros automáticos:

Figura 1: Operaciones de Cajeros

- Retirar efectivo

- Disponer de efectivo de Tarjeta de Crédito

- Transferir soles y dólares entre tus propias cuentas

- Transferir soles y dólares a otras cuentas

- Consultar tus saldos y últimos movimientos

- Pago de servicios

- Pagar Tarjeta de Crédito propias o de terceros

- Adelanto de Sueldo -

Cambiar contraseña

- Depositar a Cuentas Propias o a Terceros

Fuente: Elaboración Propia

2.2.1.4 Telecomunicaciones

Para que haya comunicación entre el terminal y la central del banco se requiere de un enlace o línea dedicada de datos que provee la empresa de Telecomunicaciones, que en este caso es Telefónica del Perú.

Se tienen las siguientes opciones determinadas por políticas del área de Telecomunicaciones de la empresa y según la disponibilidad de recursos de la ubicación:

- ADSL: También llamado “cobre” es un enlace de datos de tipo IP VPN de 20 Mbps, similar al que se tiene en los hogares pero con un ancho de banda mayor. Más utilizado para redes estáticas

- 3G: Tecnología de tercera generación conocida como IMT 2000 (International Mobil Telecommunication), es una red inalámbrica que se utiliza mayormente en sistemas móviles. Transmite aproximadamente 0.45 Mbps.

- Satelital: También llamado enlace VSAT es internet satelital de banda ancha para zonas donde los enlaces convencionales como el cobre o fibra no tienen acceso. Este tipo de enlace tiene una cobertura a nivel global, claro esta tiene un precio significativamente mayor tanto por el equipo (antena) como por el servicio y la instalación

2.2.1.5 Dispositivos de Seguridad

Para el correcto funcionamiento de un cajero automático se necesita instalar también otros elementos o dispositivos de seguridad, el objetivo es tenerlo monitoreado y en comunicación constante.

Se tienen las siguientes opciones determinadas por políticas del Área de Seguridad y Prevención de Fraudes de la empresa, sujetas a la revisión del punto y ubicación:

Los dispositivos más comunes son:

- Sensor de vibración
- Contacto magnético de puerta de bóveda
- Contacto magnético de piso
- Contacto magnético de gabinete
- Malla de protección
- Supervisión de línea de sirena
- Sirena
- Sensor de golpe de pared
- Detector de humo
- Detector de vibración y calor
- Electroimán
- Sensor de movimiento

De forma adicional cada cajero se encuentra monitoreado las 24 horas del día por una central de soporte de sistemas y otra de seguridad, adicionalmente cuenta con un contrato con empresas de seguridad que toman acción ante cualquier incidente junto a la división de Águilas Negras de la Policía Nacional del Perú.

2.2.2 Identificación en los Cajeros Automáticos

Dentro de los componentes de un cajero se encuentra el lector de banda magnética, el cual permite que el usuario ingrese una tarjeta (afiliada necesariamente a alguna de las empresas más grandes a nivel internacional como Visa, Mastercard, American Express, Plus y Cirrus) y esta lea la información que

contiene la banda magnética. En ella se encuentran los datos del usuario como nombre, cuentas y demás; esta información es solicitada por el cajero mediante el menú transaccional para que el usuario ingrese los campos y la información viaja encriptada al servidor central para hacer la validación. Si todo es conforme el usuario es identificado y entra en sesión. De acuerdo a la transacción que realice el usuario luego se hacen más validaciones como de productos, límites, montos, etc.

Más adelante es el mecanismo de dispensación el que hace el resto del trabajo para obtener los billetes de las loncheras, en el caso de un retiro, y finalmente ponerlos en la bandeja de entrega.

El método actual es bastante restrictivo ya que hay que contar necesariamente con una tarjeta de banda magnética para hacer cualquier tipo de transacción, lo cual no permite atender usuarios sin tarjeta o “no clientes”.

Según Mission ATM (2013) una transacción en un cajero automático se realiza de la siguiente manera:

1. Se introduce la tarjeta (con banda magnética o chip) en la ranura del lector y este verifica si es válida o no.
2. El sistema pasa a la siguiente pantalla donde le pregunta al cliente qué transacción desea realizar, luego le pide el ingreso de clave.
3. Los datos ingresados son encriptados y viajan al servidor central del Banco.
4. Los datos son recibidos y desencriptados.
5. A continuación se hace la validación del producto según la transacción (cuenta ahorros, corriente, tarjeta de crédito, adelanto de sueldo, transferencia, etc.)
6. Se devuelve el mensaje al cliente de la transacción y le brinda el efectivo o conformidad / disconformidad de la operación.

El proceso en ambos casos es bastante similar y se nota claramente que tienen la misma condición de uso de tarjeta de banda magnética o tarjeta inteligente.

2.2.3 Biometría

Etimológicamente el concepto biometría proviene de las palabras *bio* (vida) y *metro* (medida), por lo tanto se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

Biometric Institute, 2015 (citado por *ISO/IEC 2382-37. Information technology – Vocabulary- Part 37: Biometrics*) definió la biometría como un método automatizado de reconocimiento basado en la característica física o conductual de una persona. Entre las más utilizadas se encuentra la de reconocimiento facial, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra fisica y la transforma en una secuencia numérica, ya que tienen capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna caracteristica propia de una persona; con un determinado grado de precisión y confiabilidad.

Mite, Rodríguez & Franco (s.f., p.3) indicaron que en "un sistema de biometría tipico, la persona se registra en el sistema cuando una o más de sus caracteristicas fisicas y de conducta son obtenidos, luego es procesada por un algoritmo numérico e introducida en una base de datos. Idealmente, cuando entra, casi todas sus caracteristicas concuerdan; entonces cuando alguna otra persona intenta identificarse y no empareja completamente no le permite el acceso."

Para Vigliazzi (2006) la biometria en la seguridad de información significó la verificación de identidad de un individuo a través de una caracteristica única, esto es, el individuo será autenticado incluso si se olvida la contraseña o clave. En la figura siguiente nos aprestamos la evolución de los métodos de verificación personal.

A modo de explicación tenemos tres momentos importantes en el proceso de verificación. Inicialmente haciamos la validación con algo que sabiamos, como lo es una contraseña. Luego para incrementar el nivel de seguridad no bastaba con la clave si no que se añadió una tarjeta o smart card, junto con un dispositivo token que necesariamente tenias que traer contigo. En la actualidad podemos realizar la validación con algo que uno es como es la retina, el iris o la huella dactilar (véase Figura 8).

2.2.3.1 Tipos de biometría

Existen varios tipos de identificación biométrica, se puede realizar la identificación mediante rasgos fisicos o conductuales. Entre las de caracteristicas fisicas tenemos la huella dactilar, reconocimiento facial, identificación de iris, identificación de retina y la geometria de mano. Entre las caracteristicas de comportamiento tenemos el reconocimiento de firma y reconocimiento de voz (Vigliazzi, 2006).

Para juzgar una técnica biométrica son muchos los parámetros que hay que tener en cuenta, los más destacados según Sánchez (2000, p.15) fueron:

- Universalidad: Si las caracteristicas se pueden extraer de cualquier usuario o no
- Unicidad: La probabilidad de que no existan dos sujetos con las mismas caracteristicas
- Estabilidad: Si las caracteristicas que se extraen permanecen inalterables con relación a diversos parámetros (tiempo, edad, ritmo de trabajo, enfermedades, etc.)

- Facilidad de captura: Si existen mecanismos sencillos de captura de los datos biolOgicos o de comportamiento del sujeto
- Rendimiento: Denominado también tasas de acierto y error
- AceptaciOn: Si el usuario acepta con agrado el sistema
- Robustez: Si la técnica puede reconocer falseamiento de los datos capturados. Está técnica normalmente viene mejorada por técnicas colaterales para detectar sujeto vivo
- Costo: A la hora de implantar cualquier tipo de sistema hay que tener en cuenta el costo del mismo

Es importante mencionar que el proceso de reconocimiento se da en dos fases: primero la fase de registro o *enrollment* (véase Figura 9) y segunda la fase de reconocimiento, que a su vez tiene dos tipos. La verificaciOn de uno a uno O 1:1 (véase Figura 10) y la identificaciOn de uno a muchos O 1:N (véase Figura 11).

2.2.3.1.1 Facial

Vera (2014) indicO que este método consiste en extraer características faciales con informaciOn local (ojos, nariz, boca, etc.) y global (posiciOn de los rasgos de la cara), que se juntan para formar un modelo que puede identificarse. Esta forma está teniendo uno de los mayores crecimientos ya que se requiere una mínima inversiOn y gran expectativa.

Este tipo de tecnología se puede aplicar también en cámaras de seguridad (CCTV) o en software de reconocimiento. El proceso de reconocimiento es el siguiente:

- Captura: Utilizando patrones de video o un grupo de imágenes se mapean puntos referenciales como medidas entre por ejemplo, la posiciOn de los ojos. Aquí también entran a analizar las cámaras termales de imagen, que transmiten la temperatura del fluido sanguíneo del rostro. Estas últimas son bastantes más costosas
- ExtracciOn: El equipo convierte los padrones en un cOdigo matemático único que se almacena en un *template*
- ComparaciOn: El método más común de comparaciOn es de uno a uno (1:1), este compara el cOdigo con uno *template* almacenado anteriormente. También hay otros que pueden identificar de uno a muchos (1:N) (Klecius, 2007)

2.2.3.1.2 Iris

También denominado tecnología de identificaciOn ocular, este método es de los más jOvenes ya que data informaciOn recién desde 1997 según informO Daugman (1994). Por otro lado Biometrics (2015) indicO que el iris es un músculo dentro del ojo en forma de anillo alrededor de la pupila que controla la cantidad de luz que ingresa. Está conformado por tejidos conectivos, fibras, anillos y pigmentaciOn que

la da la melatonina. Al igual que los otros casos los rasgos del iris son únicos ya que se desarrollan en el periodo prenatal cuando antes del nacimiento se abre la pupila con sus patrones únicos. Esto es de utilidad para los fines de reconocimiento.

Se sabe que es virtualmente imposible una duplicación de este músculo ya que tiene la propiedad de desintegrarse luego de la muerte.

El proceso de reconocimiento es el siguiente:

- Captura: Se debe obtener una imagen en un ambiente muy iluminado, los lentes de contacto no interfieren en la captura de imagen pero sí los lentes oscuros. Luego de tener el iris correctamente identificado se cambia la imagen a blanco y negro para ser codificado
- Extracción: El equipo convierte los padrones en un código matemático único que se almacena en un *template*
- Comparación: La verificación uno a uno (1:1) o identificación de uno a muchos (1:N) se pueden realizar (Klecius, 2007)

2.2.3.1.3 Retina

Klesius (2007) mencionó que la retina usualmente es confundida con el reconocimiento de iris, la retina humana es un tejido de venas sanguíneas que se encuentran detrás del ojo. Al igual que el iris también tiene un patrón único que se desintegra después de la muerte.

El proceso de reconocimiento es el siguiente:

- Captura: Se debe obtener una imagen del ojo que se posiciona a unas e 3 pulgadas del lector ocular y mirar hacia un punto verde por un momento. Luego de unos segundos el lector capturará el padrón de la retina
- Extracción: El equipo convierte los padrones en un código matemático único que se almacena en un *template*
- Comparación: El método más común de comparación es el uno a muchos (1:N), este compara el código con uno *template* almacenado anteriormente (Klecius, 2007)

2.2.3.1.4 Geometría de mano

Este tipo de biometría toma una imagen de tridimensional de la mano, mide su tamaño y la longitud de los dedos y articulaciones. Es uno de los preferidos de la industria que ha sido utilizado por muchos años predominantemente para aplicaciones de control de accesos.

El proceso de reconocimiento es el siguiente:

- Captura: El usuario coloca su mano en el lector, alinea los dedos en unas guías especialmente
- Extracción: El equipo convierte los padrones en un código matemático único que se almacena en un *template*
- Comparación: El método más común de comparación es el uno a muchos (1:N), este compara el código con uno *template* almacenado anteriormente (Klecius, 2007)

2.2.3.1.5 Firma

"Uno de los sistemas biométricos más interesantes en cuestiones de seguridad y coste, es el reconocimiento biométrico de rasgos caligráficos de la firma. Mediante la recogida de firmas en tabletas que permiten establecer parámetros de presión, velocidad e inclinación del trazo se pueden obtener patrones que resultan de una gran eficacia. Estos patrones proporcionan la identidad y unidos a mecanismos de generación de firma electrónica que aportan integridad, dotan de total seguridad a firma producida mediante este procedimiento.

Los costes de implantación de esta tecnología hacen que estén al alcance de cualquier organización y hace posible la digitalización de cualquier proceso de negocio empresarial. Ya tenemos a nuestra disposición firma electrónica de documentos por parte de terceras persona sin necesidad de certificados digitales.

Por otra parte, los dispositivos de recogida de firmas no representan un coste excesivo y finalmente, el producto resultante de la firma biométrica combinada con la firma electrónica resulta en un ahorro en costes derivados del papel" (Edatalia, 2015).

Ecured (2015) indica que "el aspecto dinámico de la firma escrita es muy importante, no solo porque constituye la forma perfecta de documentar un acto voluntario, sino porque permite identificar al autor, es decir, permite unir cada firma electrónica a una única persona en concreto.

La escritura es un sistema de representación gráfica de una lengua, por medio de signos grabados o dibujados sobre un soporte. La continua automatización de los sistemas de administración de la información ha favorecido la creación de tecnologías, que permiten que sistemas automáticos realicen funciones que antiguamente llevaban a cabo personas. La aparición de equipos informáticos sofisticados que permiten el uso de lápices y punteros con interfaz de usuario ha reavivado el interés en el estudio de la escritura como objeto de reconocimiento automático.

La firma electrónica está dividida en datos estáticos y datos dinámicos, esto es según la técnica de adquisición de la firma.

- Los datos estáticos: En este tipo de firma se desprenden del trazado de la firma en dos dimensiones, y pueden revelan al grafólogo ciertos rasgos

inequívocos. Los datos dinámicos de la firma electrónica son mucho más fáciles de analizar que los datos dinámicos de la firma sobre el papel, pues los datos en soporte electrónico son exactos
- Los datos dinámicos: Sólo los datos dinámicos, la presión, la dirección, la velocidad y los cambios en la velocidad de la firma, son capaces de ofrecer una seguridad máxima en el momento de identificar una firma

Captura de la Firma: Una vez que se captura la firma manuscrita en el dispositivo esta es sometida a una etapa de acondicionamiento de la señal la cual tiene básicamente los siguientes objetivos:

- Eliminar la información que no sea relevante para el reconocimiento - Corregir la información durante la adquisición

El proceso de reconocimiento es el siguiente:

- Captura: Se debe obtener una imagen del ojo que se posiciona a unas 3 pulgadas del lector ocular y mirar hacia un punto verde por un momento, luego de unos segundos el lector capturará el padrón de la retina
- Extracción: El equipo convierte los padrones en un código matemático único que se almacena en un *template*
- Comparación: El método más común de comparación es el uno por uno, este compara el código con uno *template* almacenado anteriormente (Klecius, 2007)

2.2.3.1.6 Voz

Está tecnología está basada en el sonido de la voz. La Biometría de voz es un sistema de última generación que permite validar si la persona al otro lado del teléfono es quien dice ser. Esta validación, al tratarse de una prueba biométrica, alcanza niveles de certeza prácticamente absolutos. El proceso de reconocimiento de voz depende de las características de la estructura física del tracto vocal de un individuo así como también de sus características de comportamiento (FBI, 2015). Este sistema toma en cuenta, por un lado, rasgos físicos únicos del aparto vocal del ser humano - como su forma y tamaño - y, por otro lado, características de comportamiento como frecuencia, velocidad y acento. En conjunto estos dos aspectos generan una huella de voz digital única para cada persona.
Hay programas de reconocimiento de voz que pueden reconocer palabras, digitar letras o automatizar instrucciones pero esta no es la tecnología biométrica. Para evitar cualquier confusión con el reconocimiento de voz, los términos de reconocimiento de voz, la verificación de voz e identificación de expresión deben ser utilizados cuando se refiere a la biometría. En otras palabras, utilizar la frase "libertad de expresión" o "discurso de la identidad" en lugar de "voz".

La biometría de voz representa uno de los niveles de seguridad más altos, ya que no es algo que el usuario “recuerde” (contraseña) o “tenga” (token), si no que se define como algo que la persona “es”. Si los niveles de seguridad anteriores fueron

vulnerados, este sistema detiene un porcentaje muy cercano al 100% de los fraudes (Sixbell, 2015).

El proceso de reconocimiento es el siguiente:

- Captura: Se debe obtener el sonido de la voz mediante un micrófono
- Extracción: El equipo convierte los padrones en un código matemático único que se almacena en un *template*
- Comparación: El método más común de comparación es el uno por uno, este compara el código con uno *template* almacenado anteriormente (Klecius, 2007)

2.2.3.1.7 Huella dactilar

El reconocimiento de huella digital es el método de identificación más utilizado ya que es de fácil uso y adquisición para quien lo implementa, por ende tiene un alto grado de aceptación entre los usuarios.

La huella dactilar se obtiene de las crestas papilares de un dedo al producirse el contacto con una superficie, lo que genera una impresión o moldeado. Se basa en tres principios fundamentales:

- Perenne: Quiere decir que perdura en el tiempo. Se sabe gracias al fisiólogo checo Juan Evangelista Purkinje que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver
- Inmutable: Quiere decir que no cambia a través del tiempo. El desarrollo físico del individuo no es ningún problema para que la huella se modifique, y ni siquiera por alguna herida, corte o quemadura se afecta ya que el tejido epidérmico es capaz de regenerarse y tomar la forma original
- Único: Quiere decir que no hay otra igual, es irrepetible (Hernández, s.f.)

Si vemos un dedo podemos observar que la superficie no es lisa si no que tiene rugosidades, protuberancias y vacios en la dermis (capa exterior de la piel). Se tiene también como particularidad a las minucias, que son discontinuidades de las crestas. Se tienen más de 50 minucias en una huella digital.

Las crestas son pequeños bordes que sobresalen la piel conformados por una sucesión de papilas, son segmentos de curvas. Tenemos también los valles, que son las regiones entre dos crestas adyacentes.

Los dibujos que forman las crestas papilares son conocidos como dactilogramas, palabra derivada del griego que significa daktylos (dedos) y grammas (escrito). Los dactilogramas coinciden en que las crestas constituyen un sistema definido por su orientación, y no que sea de forma aleatoria.

Los rasgos que le dan singularidad a la huella son los cortes “core” y “delta”.El core es el extremo de la curva de una cresta, el delta es un triangulo que se forma de un conjunto de crestas.

Según el Gobierno Argentino de Biometría (2015) los tipos de información que pueden tomarse de la impresión de la cresta de fricción de una huella incluyeron el flujo de crestas de fricción (nivel 1 de detalle), la presencia o ausencia de características a lo largo de cada trayecto individual de crestas de fricción y sus secuencias (nivel 2 de detalle), y el detalle intrincado de una sola cresta (nivel 3 de detalle). El reconocimiento está usualmente basado en los primeros 2 niveles de detalle o sólo en el último.

RENIEC (2013) indicó que la tecnología AFIS (Automatic Fingerprint Identification System) “soporta la función de garantizar que las impresiones dactilares son únicas para cada persona. Así como soportar búsquedas de uno entre el universo (1:N) y autenticación de la huella muestra uno a uno (1:1).”

La plataforma del sistema AFIS, desarrollado por la empresa Morpho, está diseñado para interpretar el flujo de las crestas sobresalientes para asignar una clasificación de huellas dactilares y luego extraer los detalles de minucias- un subconjunto de la suma total de información disponible, suficiente aun para buscar efectivamente en un repositorio de huellas dactilares grande (véase Figura 12).

Los componentes del AFIS son: Codificadores, sistema de comparación 1:1, sistema de comparación 1:N, servidores de apoyo, estaciones de verificación y apoyo a peritos, equipos portátiles de verificación de identidad, equipos portátiles de identificación/verificación de identidad, estaciones de administración y gestión de excepciones y base de datos AFIS (RENIEC, 2013).

El proceso de reconocimiento es el siguiente:

- Captura: Para un proceso de identificación de uno a muchos (1:N) los individuos se registran mediante un proceso de captura óptica
- Extracción: El equipo convierte los padrones de las minucias en un código matemático único que se almacena en un *template*
- Comparación: El método más común de comparación es el uno por uno, este compara el código con uno *template* almacenado anteriormente (Klecius, 2007)

Figura 2: Proceso de identificación de huella digital

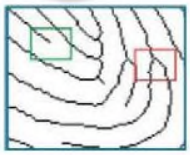
igital es capturada del lector

es pre procesada para obtener un mejor
clareza

fectos son eliminados

rísticas de la impresión son detectadas
s

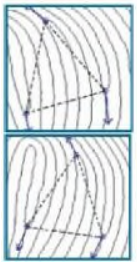
Las minucias son identificadas



Final de una papila Bifurcación

La búsqueda de las huellas en la BD se basa en
algunas de las medidas; son determinados
triángulos que conectan tres minucias. Estas
varían con la rotación y traslación.

ejada



ncontrada

Fuente: Graule, 2015 (citado por Klecius, 2007)

Debemos tener en cuenta los distintos factores que implican estos métodos biométricos y el impacto que tienen. Los factores a considerar son: nivel de precisión, facilidad de uso, barreras para atacar, aceptabilidad del usuario, estabilidad a largo plazo y estándares

Tabla 1: Comparación de métodos de sistemas biométricos

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Costo	Alto	Alto	Medio	Medio	Medio	Bajo

Fuente: Landi, C. Introducción a la biometría informática p. 20

Así mismo, es importante conocer las tasas de error (EER), falsa aceptación (FAR), falso rechazo (FRR) y fallo en el registro entre las principales técnicas biométricas. El cuadro muestra algunas cifras:

Figura 3: Comparativa tecnologías biométricas

Tipo	Físico	Físico		Físico-Compor-tamiento
Método	Activo	Pasivo	Activo	Activo
Tasa de error igual (EER)	2-3.3%	4.1%	4.1 – 4.96%	0.1 – 0.86%
Tasa de falsa aceptación (FAR)	2.5%	4%	6%	0.75%
Tasa de falso rechazo (FRR)	0.1%	10%	0.001%	0.75%
Fallo en el registro	4%	-0%	4.1 – 4.6%	0.1 – 0.86%
Coste	Medio	Alto	Muy alto	Medio - bajo
Aceptación social	Media	Alta	Baja	Alta

Fuentes: Opus Research, European Comission, IPTS

2.2.4 Autenticación Biométrica por Huella Dactilar

El objetivo de la biometría es lograr la autenticación del individuo, es decir, verificar la identidad de que la persona que está haciendo uso de un sistema es realmente la persona.

2.2.4.1 Lector Biométrico

RENIEC (2012) brindó los requisitos básicos que deben cumplir las partes. las características técnicas mínimas son:

2.2.4.1.1 Huellero Biométrico mono dactilar con lector de tarjeta inteligente integrado

- Tipo de Sensor: Óptico (CMOS o CCD)
- Tipo de Lector: Mono dactilar para captura plana de impresiones dactilares - Resolución: 500 dpi
- Área de captura mínima: 410 píxeles x 410 píxeles (a 500 dpi). El área de captura debe asegurar una resolución forense de 500dpi
- Debe incluir la funcionalidad de captura automática o no asistida de imágenes de impresiones dactilares
- El lector biométrico deberá soportar una alta carga de trabajo – Heavy Duty (ver ítem “Carga de Trabajo y Periodo de Operación”)
- Generación de imágenes en Escala de Grises de 256 tonos (8 bits), formato BMP
- El lector biométrico debe estar certificado por el FBI como dispositivo PIV SINGLE FINGER CAPTURE DEVICES y deberá aparecer listado en la url http://www.fbibiospecs.org/iafis/default.aspx (categoría “PIV SINGLE FINGER CAPTURE DEVICES”) o http://www.fips201.com/category/view/11.
- Conexión a PC por cable USB
- Compatibilidad con Sistemas Operativos Windows XP, Vista, Windows 7 como mínimo
- Deberá incluir el driver respectivo para los sistemas operativos solicitados

2.2.4.1.2 Lector de tarjeta inteligente integrado al huellero

- Soporte tarjetas ISO/IEC 7816. Debe poder leer y escribir a tarjeta Smart Card compatibles con ISO/IEC 7816. Protocolos T=0 y T=1
- Soporte PC/SC

2.2.4.2 Computador

Se requiere una máquina con la siguiente configuración mínima para poder soportar el lector biométrico:

- Procesador 32 Bits 1 Ghz.
- Memoria RAM 512 Mb.
- Disco Duro de 40Gb. con espacio de 1Gb.
- Sistema Operativo Windows XP Professional SP2
- Puerto USB 2.0
- Java 32 Bits (JRE 7u67)

2.2.4.3 Software SDK

RENIEC (2012) indicó que "el proveedor deberá proporcionar un único conjunto de Kits de Desarrollo de Software para todo el conjunto de lectores biométricos solicitados."

Cada SDK debe incluir las librerías, documentación y ejemplos necesarios para desarrollar software haciendo uso de las funcionalidades solicitadas. Las librerías deberán permitir desarrollar aplicaciones en MS NET (C++, VB) y/o JAVA.

El conjunto de SDK's deberán ser de un único fabricante. Se mencionan a continuación:

2.2.4.3.1 SDK de Captura

El proveedor debe incluir un software tipo SDK, que permita la captura de impresiones dactilares. Este SDK deberá permitir el almacenamiento de la huella capturada en formato BMP (sin compresión / 256 tonos escala de grises) o RAW.

El software debe incluir un componente para la visualización de Imágenes en vivo (visualizar en tiempo real la huella del dedo colocado sobre la superficie del lector) desde una aplicación MS Net (C++, VB) o Java, en su defecto deberá indicar a través de los ejemplos la forma de realizar la visualización en tiempo real (RENIEC, 2012).

2.2.4.3.2 SDK de Verificación de Calidad

El proveedor debe incluir software de verificación de la calidad, que permita asegurar que la impresión dactilar capturada tenga la calidad suficiente para que pueda ser utilizada en procesos de identificación con el Sistema AFIS del RENIEC, sin que afecte el desempeño del mismo, para ello deberá cumplir con las siguientes especificaciones, como mínimo:

Para la evaluación de la calidad deberá utilizar la metodología NIST Fingerprint Image Quality (NISTIR 7151) – NFIQ. En caso el software use otra metodología, el proveedor deberá indicar la equivalencia entre indicadores de calidad y los establecidos en la metodología NIST Fingerprint Image Quality (NISTIR 7151) – NFIQ. Deberá permitir que se establezcan umbrales de decisión que permitan aceptar o rechazar imágenes de acuerdo a la evaluación de la calidad de la impresión dactilar capturada (RENIEC, 2012).

2.2.4.3.3 SDK de Codificación Biométrica

El Proveedor debe incluir el software de extracción de minucias1 con las siguientes características: Extracción de Minucias a partir de la imagen capturada con el equipo biométrico, en formato estándar ANSI/INCITS 378, ISO/IEC 19794-2 COMPACT CARD (formato compacto), ISO/IEC 19794 y/o compatible con el Sistema AFIS del RENIEC.

Si el software almacena las minucias en formato estándar ANSI/INCITS 378, este software deberá ser MINEX Compliance y debe aparecer listado en http://fingerprint.nist.gov/MINEX/QPL.html categoría "MINEX Compliant Feature Extractors" (RENIEC, 2012).

2.2.4.4 Licencia

RENIEC (2012) indicó que por cada lector biométrico monodactilar se deberá incluir las Licencias run-time (en caso sea necesario), para la ejecución de las aplicaciones desarrolladas en base al conjunto de KIT's de desarrollo de software (SDK de captura, SDK de verificación de calidad, SDK codificación Biométrica).

En caso de que un único SDK proporcione todas las funcionalidades solicitadas (Captura Biométrica, Verificación de Calidad, Codificación Biométrica), se deberá proporcionar una sola licencia runtime de ser necesario, por cada lector.

La(s) licencia(s) deberán ser perpetuas, asimismo la gestión de estas deberá realizarse de manera sencilla por temas de portabilidad y facilidad de operación. Las licencias no deberán depender de archivos, números de serie, o códigos de activación que dependan de la maquina en la cual se instale o conecte el equipo, ni de llaves hardware, tokens que dificulten o impidan (por pérdida o robo) el uso del equipo y/o la respectiva licencia runtime.

2.2.5 Seguridad y Prevención de Fraudes

Según Tellez (1996, p.461) indicó que: "Los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

Lima de la Luz (1984, p.68) definió al delito informático en un sentido amplio "como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin".

Parker (1976, p.12) lo definió como "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio". Parker además define los delitos informáticos por el fin que busca:

- Propósito de investigación de la seguridad: abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973)
- Propósito de investigación y acusación: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos)
- Propósito legal: delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica

Otros propósitos: abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

La Organización de las Naciones Unidas define tres tipos de delitos informáticos – ONU (1990):

- Fraudes cometidos mediante manipulación de computadoras
- Manipulación de datos de entrada
- Daños o modificaciones de programas o datos computarizados

Entendemos entonces que el delito informático es toda acción o conducta ilícita por el uso indebido de algún medio informático en contra de un tercero, sujeta a una sanción penal.

En nuestro país mediante la ley 27309 que incorporó a los delitos informáticos en el código penal en el año 2000.

Los casos que se dan en los cajeros automáticos están relacionados a las tarjetas de crédito o débito, o algún elemento que bloquee la dispensación de efectivo. Cada vez más usuarios tienen acceso a este tipo de servicios por lo que de manera proporcional aumentan los casos de fraudes.

2.2.5.1 Clonación

Bancolombia (2015) definió a la clonación como la copia de la banda magnética de las tarjetas. Esta modalidad puede ocurrir en los cajeros automáticos o los establecimientos comerciales, al momento de retirar dinero o pagar por alguna compra.

A través de “skimming” o “clonador”: Es una técnica delictiva que utiliza tecnología avanzada, la cual permite que el ladrón pueda robar claves personales de los cajeros sin la necesidad de estar presente; todo se hace a través de un dispositivo electrónico diseñado para este fin, que permite capturar la información que hay en

las bandas magnéticas de las tarjetas, incluyendo la clave, en el mismo momento en que el usuario teclea dicha clave.

A través de “pito”: Los delincuentes tratan de abordar el cliente y con diferentes excusas buscan la manera de tomar su tarjeta; luego, con un dispositivo camuflado en diferentes elementos, rápidamente capturan la información de la tarjeta; finalmente, observan sus movimientos para identificar el número de la clave.

2.2.5.2 Trabadores

El Comercio (2015) indicó que esta modalidad consiste en una simple barra metálica que los hampones colocan en la salida del dinero de los cajeros automáticos. "Ponen fierros en la puerta por donde sale el dinero. Afortunadamente, en pocas ocasiones hemos encontrado esto adicionalmente a otros dispositivos", señaló el comandante de la policía.

Con esta regleta metálica, traban la salida de dinero y, cuando la víctima se aleja para reclamar por una falla del cajero automático, aprovechan y retiran la plata.

2.2.5.3 Cambiazo

Bancolombia (2015) también dijo sobre el cambiazo que es una modalidad de engaño a los clientes en cajeros automáticos o PAC electrónicos en cualquier situación donde la persona tenga expuesta su tarjeta para realizar una transacción.

Cuando un cliente se encuentra realizando una transacción con su tarjeta y permite ayuda de terceras personas que logran mediante engaños cambiar su tarjeta y ver su clave personal, para posteriormente realizar transacciones fraudulentas.

2.2.5.4 Suplantación

Para el caso de cajeros automáticos esta modalidad es menos recurrente. Consiste en que un estafador obtiene una tarjeta verdadera, presentando documentación falsa y haciéndose pasar por el titular (suplantación). Normalmente existe un grado de complicidad con los funcionarios de la entidad o poco control para lograrlo, de lo contrario es casi imposible pasar el filtro del trámite inicial.

De este tipo de fraude casi no se tienen

casos. **2.2.6 DNI electrónico**

El DNIe es el Documento Nacional de Identidad emitido por RENIEC “para acreditar presencial y electrónicamente la identidad de su titular, permitiendo: la firma digital de documentos electrónicos, almacenar información relativa a

la salud, programas sociales, el ejercicio del voto electrónico, verificación biométrica de la identidad sin conexión a internet, entre otras prestaciones" (Radicy s.f., obtenido de RENIEC, s.f.).

RENIEC (2012) indicó que este documento se basa en las tecnologías de firmas digitales, tarjetas inteligentes (Smart Card) y biometría, e incluirá elementos de seguridad físicos y lógicos dentro de un soporte de policarbonato, que es grabado mediante un haz de luz láser con los datos biográficos de los ciudadanos, haciendo estas características infalsificables e inviolables, permitiendo además la identificación digital y la autenticación de las personas a través del Internet.

De esta manera, permitirá acreditar la identidad del ciudadano mediante dos mecanismos:

- Físicos: Conjunto de información visible que aparece en la tarjeta, contendrá información sobre la filiación del titular, número del DNI, foto y firma del mismo, así como diversos elementos de seguridad para garantizar la integridad del documento frente a falsificaciones
- Electrónicos: Conjunto de información almacenada en el chip

Escajadillo (2009), obtenido de RENIEC (2009) indicó que estas son las principales aplicaciones y funcionalidades del DNIe:

1. Basic Access Control (BAC): Previene el acceso no autorizado al contenido del chip
2. Active Authentication (AA): Clave RSA de 1024 bits. Garantiza la autenticidad y unicidad del chip. Evita la clonación del chip ya que la clave RSA generada es única y no puede ser extraída del chip original
3. Aplicación PKI: Para el uso de los dos certificados digitales personales grabados en el chip del DNIe: Uno para autenticación (para verificar remotamente la identidad del titular) y el otro permite firmar documentos con validez oficial, como contratos
4. Aplicación Match On Card (MOC): Permite la validación de la identidad del titular mediante la comparación de la plantilla dactilar grabada en el chip y la lectura biométrica desde un lector de huellas compatible. El uso de esta aplicación también puede asociarse a la generación de la firma digital

Aplicación ICAO eMRTD: Permite una rápida lectura y toma de los datos de identidad del titular según estándar de ICAO (usado en los controles migratorios).

Figura 4: Aplicaciones que ofrece el DNIe

Fuente: Radicy (2014)

RPP (2012) señaló que “la entrega de este nuevo documento será progresiva y, a partir del 2016, cuando empiecen a caducar los DNI actuales (de color azul), la entrega será más intensiva. Para el 2021, la cobertura llegará al 79 por ciento de la población y un año después se espera que la totalidad de ciudadanos cuente con el DNIe.”

2.2.6.1 Características

RENIEC (2012) mencionó las siguientes características (véase Figura 16):

- Tamaño ISO 7810 ID1 (como una tarjeta de crédito)
- Chip con sistema operativo Java Card. Permite la incorporación posterior de aplicaciones y contenidos
- Chip con capacidad criptográfica para gestión de claves RSA y firma digital con certificados
- Memoria EEPROM de 144 Kb.
- El material de policarbonato (PC), lo que permite también la incorporación de elementos de seguridad física de última tecnología
- El material y la técnica de personalización física (grabado láser) garantizan un tiempo de vida máximo para el DNIe, superior incluso a los 8 años requeridos legalmente
- Seguridad del chip según estándares internacionales Common Criteria nivel EAL4+ ó FIPS 140-2
- SOD: Document Security Object. Firmado por el certificado Document

Signer de la CA. Es un listado con los hash de todos los DG ICAO incluidos en el chip. Confirma la autenticidad de la información contenida en los DG ICAO incluidos en el chip. Confirma la autenticidad de la información contenida en los DG ICAO

2.2.6.2 Elementos de seguridad física

Los elementos mencionados por RENIEC (2012) fueron:

- Fondo numismático
- Fondo con patrón Guilloche de líneas finas continuas, por ambas caras
- Impresión en arco iris con un mínimo de dos colores, por ambas caras
- Patrón anti-copia, por ambas caras
- Variación del ancho o distorsión de patrones de líneas finas, por ambas caras
- Microtexto con datos no variables y error deliberado, por ambas caras.
- Impresión de texto/motivo con fluorescencia ultravioleta, por ambas caras.
- Superficie lenticular vertical para la imagen láser variable
- Micro línea offset
- Zona de foto con micro texto ondulado
- Dispositivo Ópticamente Variable (DOVID)
- Grabado Láser (Laser Engraving)
- Tinta ópticamente variable (Optical Variable Ink - OVI)
- Elemento de seguridad microscópico (JDSU charms)
- Datos traslapados
- Dato variable en alto relieve como característica táctil, en el anverso.
- Imagen láser variable (CLI) (véase Figura 17)

El DNIe combina tecnologías como la de Smart Cards, personalización por grabado láser, biométrica y de firma digital.

Se denomina Smart Cards a aquellas tarjetas inteligentes con chip incrustado. El chip de que dispone el DNIe cuenta con las siguientes características según indicó RENIEC (2012):

- Chip de contactos según norma ISO/IEC 7816
- Sistema operativo Java Card. Permite la incorporación posterior de aplicaciones y contenidos adicionales
- Chip con capacidad criptográfica para gestión de claves RSA y firma digital con certificados
- Memoria EEPROM de 64 Kb.
- Seguridad del chip según estándares Common Criteria nivel EAL4+ ó FIPS 140-2

2.2.6.3 Tecnología biométrica

RENIEC (2012) indicó que el DNIe ofrece a través de su aplicación Match-on-Card una autenticación por tecnología biométrica. El proceso se realiza de la siguiente manera:

- Dentro del proceso de inscripción de los ciudadanos se toma sus huellas dactilares (enrolamiento)
- A las imágenes de las huellas se les extrae las minucias y se obtienen las plantillas biométricas
- Las plantillas biométricas de ambos dedos índices se almacenan en el chip
- Para la validación de la identidad del ciudadano, al acercarse éste a un punto de atención coloca su índice sobre un lector
- El equipo extrae las minucias que caracterizan a la huella en particular y genera una plantilla biométrica
- Esta nueva plantilla biométrica es enviada a la aplicación Match-on-Card, la que la compara con la original que fue guardada durante el enrolamiento y que pertenece al ciudadano titular del documento
- La propia aplicación Match-on-Card de la tarjeta da la respuesta en cuanto a si ambas plantillas corresponden o, lo que es lo mismo, valida la identidad

La aplicación Match-on-Card cuenta con parámetros de operación idóneos en lo que se refiere a tiempo de respuesta, tasa de falsa aceptación, tasa de falso rechazo e igualmente en cuanto a su operación dentro de los estándares tecnológicos vigentes.

2.2.6.4 Legislación

RENIEC (2012) indicó sobre la ley N˚ 27269, “Ley de Firmas y Certificados Digitales. Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante Decreto Supremo N° 052-2008-PCM, modificado mediante Decreto Supremo N° 070-2011-PCM.“

Congreso de la República (2012) indicó la LEY DE FIRMAS Y CERTIFICADOS DIGITALES

“Artículo 1º.- Objeto de la ley La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 2°.- Ámbito de aplicación La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos. DE LA FIRMA DIGITAL.

Artículo 3°.- Firma digital La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. DEL TITULAR DE LA FIRMA DIGITAL.

Artículo 4°.- Titular de la firma digital El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5°.- Obligaciones del titular de la firma digital El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas. DE LOS CERTIFICADOS DIGITALES.

Artículo 6°.- Certificado digital El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.
Artículo 7°.- Contenido del certificado digital Los certificados digitales emitidos por las entidades de certificación deben contener a l menos: 1. Datos que identifiquen indubitablemente al suscriptor. 2. Datos que identifiquen a la Entidad de Certificación. 3. La clave pública. 4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos. 5. Número de serie del certificado. 6. Vigencia del certificado. 7. Firma digital de la Entidad de Certificación. “

2.2.7 Gerencia de Canales Electrónicos

La Gerencia de Canales Electrónicos compete tanto la gestión de los productos ATMs o cajeros automáticos y de la plataforma virtual o kiosko.

2.2.7.1 Misión

Atender de manera eficiente las transacciones de nuestros clientes, ofreciéndoles calidad, conveniencia, seguridad y productos y servicios basados en sus necesidades.

2.2.7.2 Visión

Ser los puntos de contacto más relevantes para nuestros clientes y usuarios en su experiencia con el Banco.

2.2.7.3 Organigrama

Figura 5: Organigrama

Fuente: Área de Canales Alternativos

El área tiene comunicación con diversas unidades que le dan servicios. Se mencionan las principales y sus funciones:

- Gestión de Efectivo: Traslado de valores
- Centro de Monitoreo: Central de Monitoreo / Soporte técnico
- Gestión de Información: Datawarehouse
- Ingeniería y desarrollo tecnológico: Proyectos de desarrollo del sistema
- Marketing: Comunicaciones y publicidad
- Telecomunicaciones: Comunicación
- Seguridad y Prevención de Fraudes: Seguridad física
- Ingeniería: Obras civiles
- Post-venta: Reclamos, casos varios
- Administración de Riesgo Operativo: Gestión del Riesgo
- Activo Fijo: Pagos y alquileres
- Legal: Contratos

2.2.7.4 Funciones

Las siguientes funciones son dadas por la Gerencia de Canales Alternativos:

- Elaborar propuestas y modelos para el dimensionamiento de la capacidad instalada de los canales a su cargo en función al potencial y crecimiento económico de la plaza, así como nuestra posición frente a la competencia. Estas propuestas se realizan anualmente y/o

puntualmente e incluyen propuestas sobre instalación, desinstalación y reubicación de ATMs y plataforma virtual

- Buscar el incremento de la rentabilidad de los diferentes canales electrónicos: Cajeros automáticos, plataforma virtual de Atención y puntos de venta (POS), en función a la optimización de su uso, derivación de operaciones a canales más rentables y la implementación de nuevas funcionalidades para el cliente que permitan un mayor uso de la capacidad instalada de los medios electrónicos así como la venta y/o promoción de productos a través de los mismos

- Desarrollar proyectos y elaborar propuestas integrales que busquen mejoras en los servicios y funcionalidades que se prestan actualmente en los canales electrónicos, efectuando un análisis costo beneficio, a fin de determinar su rentabilidad y conveniencia para el Banco

- Coordinar y priorizar con las Gerencias de Área involucradas (Infraestructura, Sistemas, Administración de Efectivo, Seguridad, Prevención de Fraudes, etc.) el desarrollo e implementación de los proyectos propuestos, liderando la ejecución de los mismos y efectuando el seguimiento correspondiente

- Elaborar el presupuesto anual de ingresos, gastos e inversión de los canales electrónicos y llevar a cabo su seguimiento y control

- Evaluar e implementar las alternativas referentes al diseño de la imagen y a la señalización de los canales electrónicos

- Velar por la disponibilidad y operatividad diaria de los canales electrónicos, en coordinación con las Gerencias de Área involucradas en los distintos procesos asociados (Seguridad, Centro de Monitoreo., Sistemas, Administración de Efectivo, Seguridad, Prevención de Fraudes, etc.) llevando a cabo las medidas pertinentes para su mejora continua.

- Coordinar con la Gerencia de Área encargada las condiciones de alquiler y disposición de espacios para la ubicación de los Cajeros Automáticos en sus locales o dependencias, bajo parámetros, estándares y criterios costo/beneficio coordinados con las gerencias de la Gerencia de División de Marketing y Responsabilidad Social y la Gerencia de División Comercial

- Diseñar los diferentes reportes para una mejor gestión de los canales electrónicos y toma de decisiones con respecto a ellos

- Realizar otras labores que se le asignen relacionadas a los canales electrónicos

2.2.8 Información Canales Alternativos

A continuación se mostrará información de los distintos canales de

atención. **2.2.8.1 Benchmark**

Los niveles de transacciones monetarias en los distintos canales de atención muestran claramente la migración transaccional de canales los canales tradicionales como ventanilla hacia los alternativos como agente o cajeros automáticos (véase Gráfico 1).

También hay un gran porcentaje de transacciones que se realizan con instrumentos distintos al efectivo (véase Gráfico 2). Está gráfica muestra información de todos los operadores a nivel nacional. Se aprecia claramente que el canal cajeros automáticos tiene un gran porcentaje de operaciones sin cash, le sigue los terminales de punto de venta. En menor proporción está el canal agente y otros. Según la revista digital Con Nuestro Perú (2015), obtenido de ASBANC (2015), en el artículo “Internet: canal moderno que facilita las transacciones financieras” indica que “considerando los datos del primer bimestre del último año, se verifica que el canal más utilizado para efectuar estas transacciones estuvo conformado por los Cajeros Automáticos, Monederos y Multifuncionales (que concentró el 36.24%), seguido por Terminal Punto de Venta – POS (22.80%) y Cajero Corresponsal (14.04%). En el 2014 también destacó el uso del Ventanilla (con un 7.41%), seguido de Software Corporativo1 (5.97%) y Banca por Internet (5.95%)” (Véase Gráfico 3).

En el Gráfico 4 tenemos una gráfica que muestra la comparación entre las entidades respecto a las transacciones totales que se realizan en todos los canales. Hay una gran diferencia de participación del mercado del BCP y el resto.

En el Gráfico 5 se muestran las transacciones totales por canal de las principales entidades financieras, se aprecia la proporción de operaciones que tiene cada canal respecto al todo. La ventanilla y cajeros automáticos ocupan gran proporción en todos.

En los últimos años el canal que ha tenido un crecimiento mayor es el canal corresponsal o agente, que ha crecido siete veces desde el 2008 (véase Gráfico 6).

2.2.8.2 Información Cajeros Automáticos

Lima concentra el mayor porcentaje de cajeros automáticos a nivel nacional y en mucho menor grado las distintas provincias resaltando el norte y el sur andino (véase Gráfico 7).

Los cajeros se encuentran segmentados por ubicación, el mayor porcentaje se encuentran instalados en las agencias a nivel nacional, luego tenemos las ubicaciones retailers como los centros comerciales, supermercados, estaciones de servicio, boticas, entre otros. También tenemos otros tipos de ubicaciones como aeropuertos, centros de salud, centros de estudio, halls, hoteles, clubs, etc. Finalmente tenemos los cajeros instalados en empresas (véase Gráfico 8).

El banco trabaja actualmente con dos grandes marcas (Diebold y NCR) pero la renovación tecnológica o cambio de modelo que se hace es a los modelos Diebold. Se muestra en el Gráfico 9 el porcentaje de una marca frente a la otra.

También es importante mostrar los cajeros que se tienen tanto de depósito como de retiro. Como se aprecian en el Perú la gran mayoría son cajeros de retiro pero el parque de cajeros de depósito está incrementando cada vez. Actualmente estos cajeros solamente son instalados en las agencias, más no fuera de ellas (véase Gráfico 10).

Referente a los modelos actualmente se cuentan con 12 pero estos modelos se agrupan por familias que son básicamente los mismos modelos con modificaciones como la posición de la bóveda para el abastecimiento (posterior o frontal) o si son de pared o lobby. Bajo este criterio se están colocando en 4 grupos de familias (véase Gráfico 11).

3.1 Definición Operacional de las Variables

Tabla 2: Definición operacional de variables

Variables	Dimensiones	Ítem	Tipo de Variable	Valor	Indicador	Técnica	Instrumento
Biometría mediante huella dactilar	Seguridad	1	Cualitativo	1: mínimo 2:ligero 3:básico 4:regular 5:avanzado	Controles de seguridad	Análisis	Reportes
	Estratégico	2	Cuantitativo		Proyección transaccional	Método Sarima	Reporte
Red de Cajeros automáticos	Competitividad	3	Cualitativo		Ranking bancario / Funcionalidades	Análisis	Reporte

Fuente: Elaboración propia

3.2 Diseño tipo y enfoque de estudio

El presente proyecto será una investigación aplicada de tipo descriptiva en la primera parte ya que describiré los fenómenos tal como se presentan en la realidad sin manipular variables, y explicativa en la segunda parte ya que se busca el por qué de los hechos así como establecer las relaciones causa – efecto. Tendrá un diseño no experimental con enfoque cualitativo - cuantitativo.

3.3 Población y Muestra

3.3.1 Población

El parque total, que es nuestra población, es de 2260 cajeros automáticos (información a julio del 2015). Respecto a las transacciones tenemos el total de transacciones de todos los canales de los últimos 4 años hasta el mes de julio del presente año.

3.3.2 Muestra

Nuestra unidad muestral para la presente investigación será el cajero automático como unidad. Utilizaremos un muestreo no probabilístico intencional para poblaciones finitas.

Inicialmente afectará a 233 cajeros que son los cajeros de depósito. Por un tema de facilidad en las coordinaciones, control del despliegue y reclamos se realizará en la red de agencias.

Para el tema transaccional solamente utilizaremos el total de transacciones del canal ATM desde el 2011.

3.3.3 Criterios de Inclusión

Todo el parque de cajeros de depósito que esté operativo o activo. Tener en cuenta que hay agencias que cierran por remodelación, por temas del propietario (en el caso de inmuebles alquilados) o por problemas municipales.

3.3.4 Criterios de Exclusión

Cajeros que por alguna razón, como el proceso de cambio de modelo o algún otro incidente del ambiente, no estén disponibles. El estado de estos es pendiente, si está retirado momentáneamente o algo evita su funcionamiento en un período mayor a un mes; y el otro estado es inactivo cuando se trata de un nuevo cajero que está próximo a ser instalado.

3.4 Técnicas de recolección de datos

Utilizaremos la técnica llamada análisis documental que constituye el punto inicial o más importante de la investigación ya que los principales documentos fuentes que utilizaremos son reportes provenientes de la institución bancaria, estudios de mercados, benchmark y teorías ya aplicadas. Toda esta información será procesada y analizada.

3.4.1 Instrumentos

3.4.1.1 EViews

Fue desarrollado por Quantitative Micro Software, es un software estadístico hecho para Windows que se utiliza básicamente para el análisis econométrico. El programa es compatible con los principales paquetes estadísticos del mercado como lo son Excel, SPSS, SAS y Stata.

3.4.1.1 ICaiken

El programa ICaiken es un software desarrollado por Merino & Livia en Visual Basic y hecho para Windows. Es un programa muy sencillo e intuitivo donde solamente basta ingresar los valores para que se haga el cálculo.

3.5 Procedimiento para la elaboración del diseño

3.5.1 Diseño del flujo y adecuación de usos del DNIe

Se deberá hacer el análisis para el nuevo flujo sobre el proceso de acceso a los cajeros automáticos y las variables que entran en esta interacción.

Respecto al DNIe se revisarán cuales son las bondades y características de los usos que tiene y cuales aplican para los fines de este estudio, teniendo en consideración las limitaciones tecnológicas o de infraestructura.

3.5.2 Análisis de información

Se hará un análisis respecto a la información de las transacciones y de los distintos canales. Aquí utilizaremos los programas EViews e ICaiken.

3.6 Técnicas de procesamiento de información de los datos

Tenemos la información histórica de las transacciones en el canal de los últimos 4 años y vemos que uno de los modelos que mejor aplicaría es SARIMA ya que son los que se adecuan a series con este tipo de comportamiento. Muestra un

comportamiento estacionario (se observa en los picos) y de tendencia (debido al crecimiento), además de poseer una media móvil (la media o promedio varía según el registro de nuevas transacciones).

3.6.1 Modelo Sarima

Según Ferrero (2011**)** muchas series temporales no son estacionarias, ya sea porque presentan tendencias o por efectos estacionales. Específicamente, muchos tipos de series, no son estacionarias pero pueden convertirse en series estacionarias utilizando la diferenciación de primer orden. Como la serie diferenciada necesita ser agregada (o integrada) para recuperar la serie original, el proceso estocástico subyacente se llama media móvil integrada autorregresiva (ARIMA).

Los procesos ARIMA se pueden desarrollar para incluir términos estacionales, abriendo camino a modelos ARIMA estacionales no-estacionarios (SARIMA) de sus siglas en inglés (*seasonal autoregressive integrated moving average*).

Según Chávez (1997) los modelos SARIMA captan una conducta puramente estacional de una serie, se realiza para la componente regular o no estacional. Una serie con influencia solamente por la componente estacional puede ser descrito por un modelo SARIMA (P,D,Q), el cual se lo representa de la siguiente manera:

Donde la constante μ es el nivel del proceso original $\mathbf{Z_t}$.

Es un polinomio autorregresivo estacional de orden **P**.

Es un polinomio de promedios móviles estacional de orden **Q**.
$\mathbf{a_t}$: Es un proceso de ruido blanco (es una señal no correlativa, es decir, en el eje del tiempo la señal toma valores sin ninguna relación unos con otros).

Como es de esperar en la práctica no siempre se presentan series con componente regular únicamente, o afectadas por la estacionalidad solamente; sino por el contrario, generalmente se presentan series afectadas por ambas componentes, tendencia regular y estacionalidad. En este sentido Box y Jenkins (1970) propone un modelo denominado multiplicativo, el cual puede explicar el comportamiento de una serie afectada por ambas componentes.

En resumen López (2013) indica que es autorregresivo e integrado de promedio móvil estacional, se basa en ARIMA, con algunos de sus coeficientes en cero y componentes adicionales para integrar el comportamiento estacional de la serie. SARIMA tiene la siguiente notación:

$$\Phi_p(L)\Phi_p(L)\left(1-L^s\right)^D(1-L)^d(Y_t-\mu)=\Theta_Q(L)\Theta_q(L)u_t$$

La notación utilizada es la siguiente:

Yt: serie de tiempo que será analizada
ut: función de blanco con promedio cero y varianza constante
dyD: grados de diferenciación normal y estacional
$\Phi_p(L)$: polinomio de orden p del componente autorregresivo
$\Phi_p(L)$: polinomio de orden P del componente estacional autorregresivo
8_q: polinomio de orden q del componente de medias móviles
$8_Q(L)$: polinomio de orden Q del componente estacional de medias móviles
S: periodo de la función si presenta estacionalidad
p: promedio de la función original sin diferenciar

Concepto de estacionalidad y sus tipos según López (2013):

1. Una serie estacional presenta valores que no son constantes pero varían con una pauta cíclica. Cuando E[Xt]=E[Xt+s] decimos que s es el período de estacionalidad, y éste limita el número de observaciones que forman el ciclo estacional: s=12 (serie mensual), s=4 (trimestral), s=7 (semanal)

2. El modelo más simple trata un efecto constante que se suma a los valores de la serie: Xt=St+nt. La serie se escribe como suma de un componente estacional St y un proceso estacionario nt (con mu su media)

3. El componente estacional St puede tener comportamiento:

   - Determinista (función constante para el mismo mes en distintos años) St=St+ks
   - Estacionario (evoluciona en el tiempo y su evolución es estacionaria, oscilando alrededor de un valor medio) St=mu+vt, donde vt es un proceso estacionario de media cero que introduce variabilidad en el año, o 3= no-estacionario (es cambiante sin ningún valor medio fijo) St=St-s+vt

3.6.2 Coeficiente V de Aiken

Según Merino & Livia (2009, p.169) indicaron que “un método aparentemente más difundido es el coeficiente V de Aiken (Aiken, 1980; 1985). Este coeficiente es uno de los métodos para cuantificar la validez de contenido o relevancia del ítem

respecto a un dominio de contenido en N jueces. El valor de V va desde 0.00 a 1.00, en que 1.00 es la mayor magnitud posible que indica un perfecto acuerdo entre los jueces respecto a la mayor puntuación de validez de los contenidos evaluados. La interpretación del coeficiente usa la magnitud hallada y la determinación de la significancia estadística mediante las tablas de valores críticos; estos se hallan en Aiken (1985). La ecuación, algebraicamente modificada por Penfield y Giacobbi (2004) es:

$$V = \frac{\bar{x} - l}{k}$$

$\bar{x}$ media de las calificaciones de los jueces en la muestra
l calificación más baja posible
k rango de los valores posibles de la escala Likert utilizada.
Por ejemplo, si l = 1 y k = 5, entonces k = 5 – 1 = 4."

$$L = \frac{2nkV + z^2 - z\sqrt{4nkV(1-V) + z^2}}{2(nk + z^2)}$$

Respecto a los intervalos de confianza Merino & Livia (2009, p.170) indicaron que "al tratar la V de Aiken como una proporción, la construcción del intervalo en un nivel de confianza determinado se presenta en las siguientes ecuaciones:

Para el límite inferior del intervalo:

$$\frac{2nkV + z^2 - z\sqrt{4nkV(1-V) + z^2}}{2(nk + z^2)}$$

Para el límite superior del intervalo:

$$\frac{2nkV + z^2 + z\sqrt{4nkV(1-V) + z^2}}{2(nk + z^2)}$$

L límite inferior del intervalo
U límite superior del intervalo
Z valor en distribución normal estándar
V V de Aiken, calculado por la primera fórmula

continuación. El intervalo de confianza para la V de Aiken creado lleva al usuario a probar si la magnitud obtenida del coeficiente es superior a una que es establecida como mínimamente aceptable para concluir sobre la validez de contenido" (Merino & Livia , 2009, p.170).

Agregando a lo indicado por los autores citados anteriormente Escurra (1989) indicó que el uso de la V de Aiken como criterio para establecer la validez de un

instrumento en función al acuerdo entre jueces expertos está enfocado en retener aquellos reactivos que tienen una V de 0.50 a más. Es por ello que el cálculo de los intervalos de confianza es necesario, dado que no se puede tomar como un indicador exacto aquella estimación cuantitativa realizada de una característica estudiada.

CAPÍTULO IV. RESULTADOS

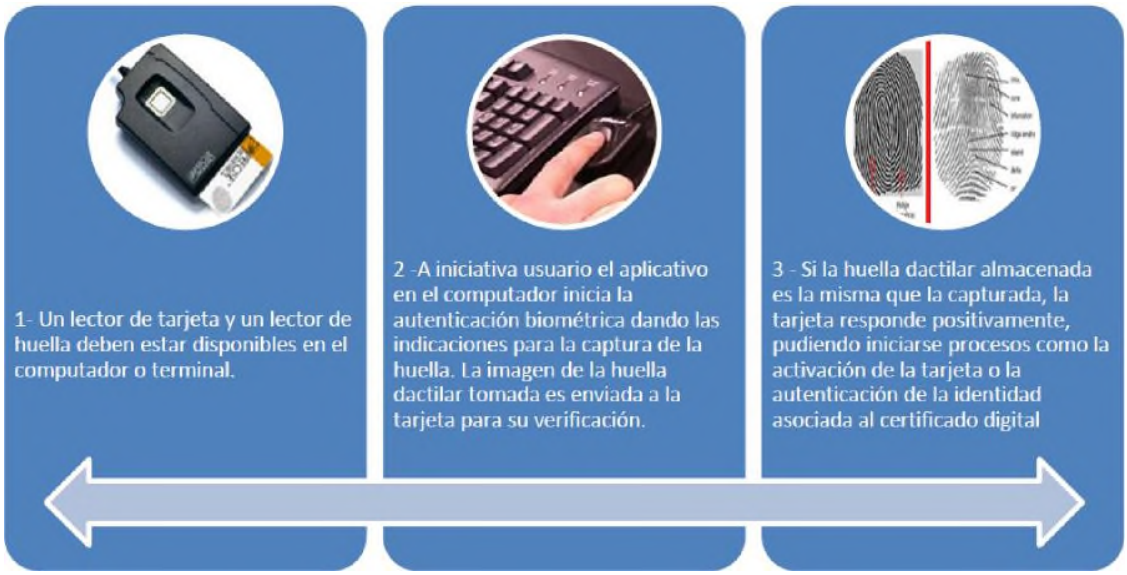
4.1 Acceso al ATM con el DNIe

Dentro de la extensa lista de usos que RENIEC dio para el DNIe hay dos usos en particular que nos interesan para fines de esta investigación. Son los siguientes:

4.1.1 Proceso de autenticación con la aplicación Match On Card

Cumplimos con los requerimientos para que se dé el proceso de autenticación ya que contamos con un lector de tarjeta inteligente en el cajero. Adicionalmente se adquiere un lector biométrico de huella digital.

Figura 6: Proceso de autenticación con aplicación MOC



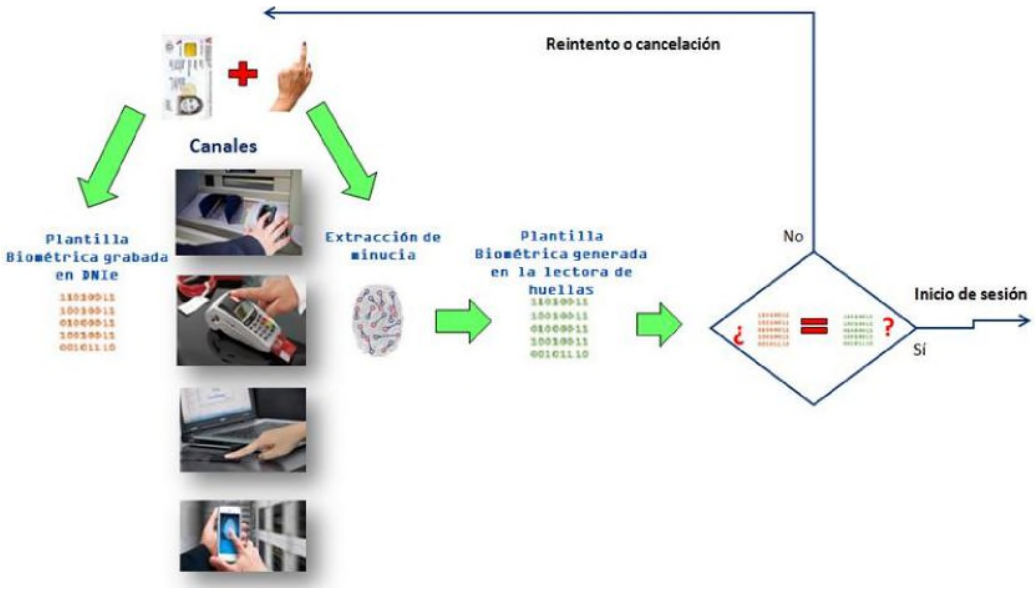
Fuente: RENIEC (2012)

- Para dar acceso privado a bases de datos, aplicaciones informáticas, entre otros. En nuestro caso a servicios bancarios
- Valida la identidad de la persona: Solicitando la lectura del DNIe y el ingreso del PIN respectivo para acceder al certificado digital de identificación, o mediante la verificación de la huella dactilar, mediante “Match On Card”

Con la aplicación Match On Card la comparación se realiza entre la información de la huella digital almacenada en la smart card (tarjeta inteligente) y la huella digital que uno colocó en el lector de huella digital. A continuación se inicia con la autenticación y la imagen de la huella obtenida se envía a la tarjeta para ser

verificada. Si el resultado es positivo inicia la transacción. La figura muestra el proceso.

Grafico 14: Flujograma - Autenticación con el DNIe (mediante Match On Card)



Fuente: Área de Canales Electrónicos

Se considera para este estudio el lector biométrico marca Lumidimg modelo Voyager V31x ya que este lector ha sido recomendado por nuestro proveedor Diebold. Cumple con los requerimientos necesarios para nuestro objetivo y tiene casi las mismas especificaciones que el lector Safran Morpho certificado por RENIEC.

Tabla 3: Comparación lectores biométricos

Ítem	Especificación técnica	
Marca	SAFRAN MORPHO	LUMIDIMG
Modelo	MSO300	Voyager V31x
Tipo de sensor	Óptico	Óptico
Tipo de lector	Mono dactilar	Mono dactilar
Resolución	500 dpi	500 dpi
Área de captura	410 píxeles x 410 píxeles (a 500 dpi)	352 píxeles x 544 píxeles (a 500 dpi)
Soporte	Alta carga	Alta carga
Escala de grises	256 tonos (8 bits)	256 tonos (8 bits)
Conexión a PC USB	Sí	Sí

Compatibilidad S.O.	WXP, W7 y W8	WXP, W7, W8 y Linux

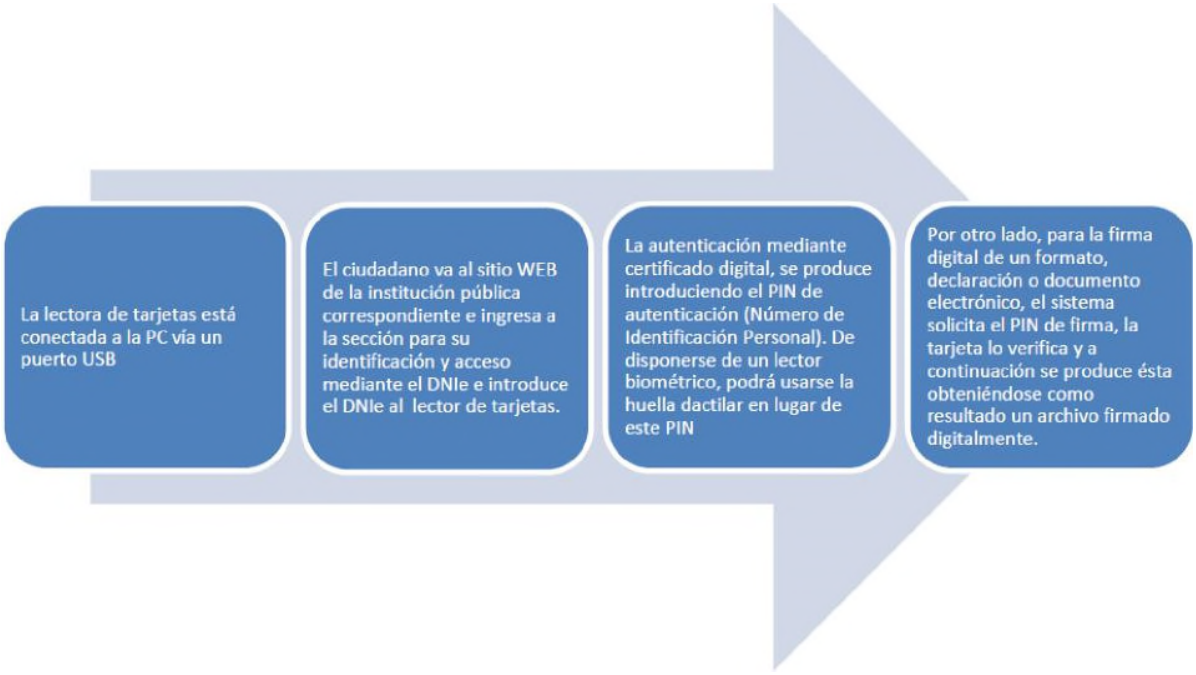
Fuente: Elaboración propia

Respecto al software Verifinger SDK lo estamos utilizando de igual manera por recomendación de nuestro proveedor Diebold. Este también cumple con los requisitos mínimos del hardware.

4.1.2 La firma digital

Así mismo utilizaremos también la bondad de la firma digital

Figura 7: Proceso de firma digital



Fuente: RENIEC (2012)

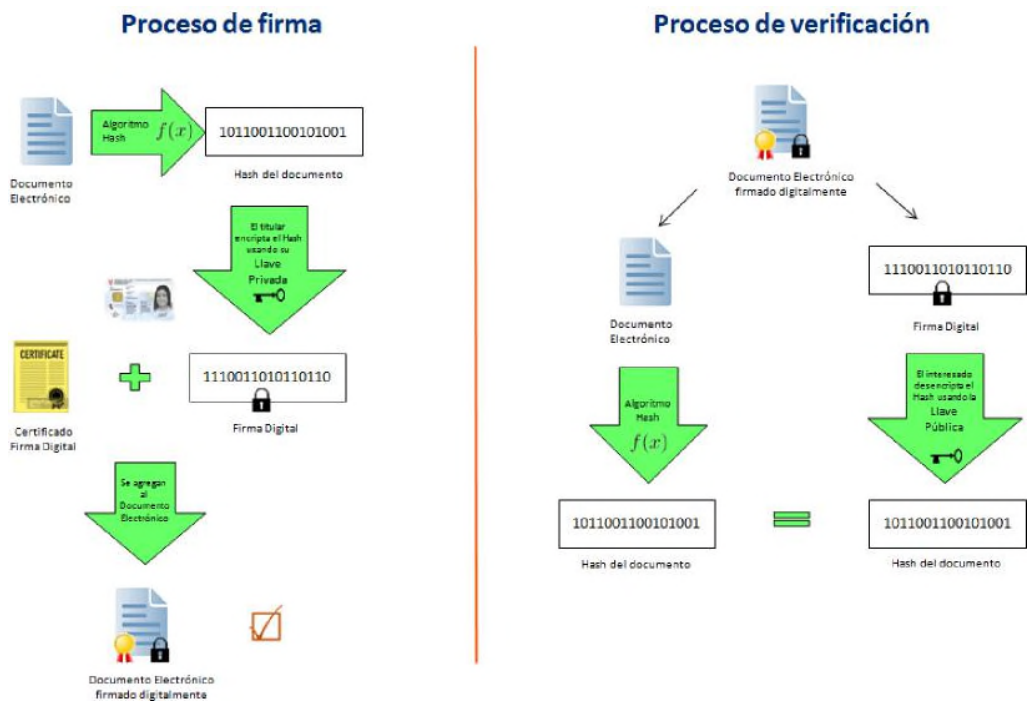
- Se aplica a un documento electrónico (formulario, contrato, carta, solicitud, etc.) quedando grabada como parte de el
- Deja constancia de que el firmante es el autor o está de acuerdo con lo expresado en el documento
- Garantiza que la información del documento no será alterada. Para ello el firmante hace uso del PIN de su DNIe para acceder a su llave privada y aplicar el certificado digital de firma

Se mencionan algunos conceptos para aclarar mejor el proceso según el glosario de RENIEC (2012):

- Firma digital: Es un dato digital adjunto, lógicamente asociado a un documento digital. Permite identificar a la persona que firma, vincular al documento con la persona que lo firma y preservar la integridad del documento firmado (evitar la alteración)
- PIN: Secuencia de caracteres numéricos que permiten el acceso a la llave privada asociada a los certificados digitales grabados en el chip del DNIe
- Llave privada: Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital
- Llave pública: Es la otra clave en un sistema de criptografía asimétrica que es usada por cualquier interesado en verificar la validez de la firma digital puesta en un documento. La clave pública puede ser conocida por cualquier persona y es puesta a disposición pública por RENIEC
- Certificado digital de firma: Documento digital emitido por una Entidad de Certificación (EC). Vincula la identidad física de una persona con su firma digital

Algoritmo Hash: Función matemática que resume el contenido de una cadena alfanumérica en una representación codificada única.

Gráfico 15: Flujograma - Funcionamiento de la firma digital



Fuente: Área de Canales Electrónicos

Hay muchos beneficios de utilizar la firma digital en lugar de la firma manuscrita, la digital es única cada vez que se genera mientras que la manuscrita siempre es la misma. Por otro lado la firma manuscrita es falsificable, es sumamente sencillo hacer una réplica de una firma. Así mismo es repudiable, es decir, que puede ser rechazada por el supuesto autor; y por último no garantiza la integridad de los datos. Al ser un documento en cualquiera de las partes de un proceso por ejemplo se puede agregar o quitar algo, por lo que ya no es integro el documento.

El cuadro muestra las ventajas antes mencionadas y describe las particularidades entre la nueva firma digital y la firma manuscrita que actualmente se utiliza.

Figura 8: Firma manuscrita vs Firma digital

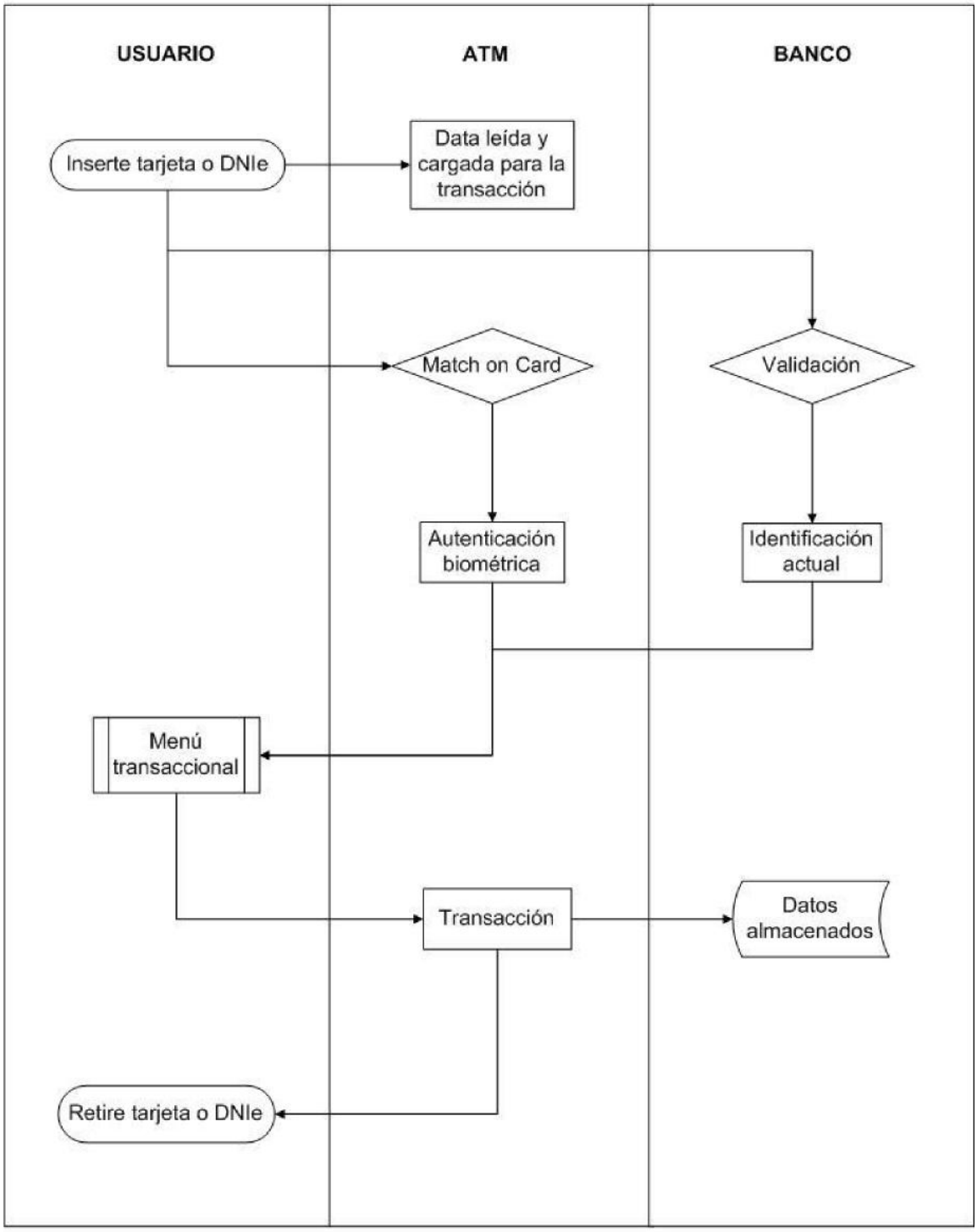
Firma manuscrita	Firma digital
	
La misma "siempre"	Única cada vez
Falsificable	Infalsificable
Repudiable	No repudiable
No garantiza integridad de datos	Garantiza integridad de datos

Fuente: Área de Canales Electrónicos

El proceso que se tiene actualmente se mantuvo ya que muchos de nuestros clientes lo siguen utilizando sea por costumbre o porque aún no cuentan con el nuevo DNIe. El MOC generó a su vez un nuevo proceso de negocio ya que la información de los "no clientes" es almacenada para que también sea procesada, de esta manera podemos entender mejor el habito de ellos y a su vez ofrecerles productos que estén más a su medida.

Se grafica como quedó el nuevo proceso que incluye el MOC.

Gráfico 1: Flujograma - Nuevo Proceso de Negocio



Fuente: Elaboración propia

Esta imagen muestra donde fue ubicado el huellero en un cajero automático. El ATM cuenta con un espacio disponible al costado del teclado donde se instaló el lector biométrico.

Figura 9: Lector biométrico en ATM Diebold

Fuente: Diebold (2014)

Se mostró que la aplicación MOC se adecua al proceso de identificación de los cajeros automáticos y se suma a este la firma digital para poder hacer uso del certificado digital.

4.2 Seguridad y Prevención de Fraudes

Respecto a la seguridad y la prevención de fraudes la implementación de la biometría mediante huella digital evitará los casos de clonación, cambiazo y suplantación ya que la huella es única para cada persona, y requiere necesariamente la presencia del usuario durante la transacción en el cajero para autenticar. Así mismo, se necesita tejido vivo ya que el lector biométrico detecta la presión sanguínea, esto evitará que personas no autorizadas intenten hacer moldes con huellas para cometer fraude.

Por la parte de facilidad esta tecnología no requerirá que el usuario sepa o recuerde su clave, esto facilitará mucho a personas de la tercera edad que constantemente olvidan tanto la tarjeta de crédito o débito como la contraseña.

De cara al cliente tenemos estas las siguientes ventajas que se muestran en el cuadro:

Tabla 4: Comparación identificación actual vs autenticación biométrica

Tipo de Fraude	Identificación actual	Autenticación biométrica por huella digital
Clonación	Si el cajero no cuenta con sensor de movimiento puede ser vulnerado	Imposible de vulnerar al momento
Trabadores	Si el cajero no cuenta con sensor de movimiento puede ser vulnerado (modalidad no vigente)	Si el cajero no cuenta con sensor de movimiento puede ser vulnerado (modalidad no vigente)
Cambiazo	Si se consigue la contraseña del usuario se lleva a cabo	Imposible de vulnerar al momento
Suplantación	El cajero actual es incapaz de reconocer un fraude por esta modalidad	Imposible de vulnerar al momento

Fuente: Elaboración propia

De cara al banco tendremos menores gastos operativos ya que la validación de identidad se hace en el punto, sin necesidad de conectarse a bases centralizadas para comparar huellas, claves y/o tarjetas. Con esto se mostró cualitativamente la reducción de las vulnerabilidades de seguridad del proceso de identificación actual.

Hacemos un pequeño ejercicio para simular los gastos que normalmente se tienen para sistemas como consulta RENIEC o centrales de riesgo. El costo por consulta es s/. 0.48 por transacción, por volumen.

Figura 10: Costo del servicio consulta RENIEC (línea dedicada)

Rango de consultas	Tasa por consulta
0 - 200,000	S/. 0.90
200,001 - 400,000	S/. 0.68
400,001 - 600,000	S/. 0.48
600,001 - 800,000	S/. 0.31
800,001 - A MAS	S/. 0.19

Fuente: RENIEC

Como dato de la División Comercial tenemos que las consultas son alrededor de 400,001 al año y lo multiplicamos por s/.0.48, tenemos s/. 192,000.48 en gastos para este tipo de validación. El MOC permite hacer la validación en el punto por lo que estos gastos no son necesarios. A modo de dar un mayor sustento se coloca el ejemplo del caso de éxito del Banco Supervielle que implementó la biometría:

Según Bolo (2015), Director de Tecnología de IBM, indicó que trabajó junto al Banco Supervielle para mejorar su modelo de atención al cliente que estaba enfrentándose a un nivel de fraude importante. Ante esto aplicó la técnica biométrica más tradicional que es la huella digital que permitió a las personas simplificar los trámites y reducir el tiempo de espera. La biometría se aplicó inicialmente para el proceso de pago de fondos de las jubilaciones y pensiones.

También indicó que este Banco ya cuenta con más de 700 clientes afiliados al sistema, y como resultado ha dejado demostrado que se redujo un 70% el tiempo de espera de los jubilados. A su vez le permitió optimizar indicadores clave de rendimiento y realizar análisis de crédito y puntuaciones en línea. La apertura de nuevas cuentas pasó de 11 días a 20 minutos y, para las tarjetas de crédito, de 30 a 2 días. Además, el banco disminuyó en un 20% sus costos de operación, aumentó en un 70% la eficiencia en la distribución de documentos y redujo del 50% al 5% las transacciones que requieren la intervención humana para apertura de créditos y puntuación de clientes, lo que permite relocalizar sus recursos en tareas más estratégicas.

Sobre el mismo caso Gustavo Bauso (2014), CIO del Banco Supervielle, indicó que tras el crecimiento sostenido del banco se vieron obligados a incursionar en la biometría. Los resultados son concretos, aseguran que han mejorado los tiempos de atención en la red de sucursales, han bajado los costos operativos del banco y les dieron a los usuarios una aplicación fácil de operar, dando así una plataforma más robusta e integrada.

4.3 Competitividad

A nivel de funcionalidad hay una competencia entre los principales bancos por dar más y mejores servicios. La implementación de la biometría traería consigo poder dar más servicios que actualmente no se dan por un tema regulatorio (funcionalidades ya implementadas pero restringidas). Tener en cuenta que por regulación de la Superintendencia de Banca y Seguros (SBS) actualmente el banco en estudio no realiza transferencias interbancarias para evitar el lavado de activos al no poder identificar al usuario ordenante, de igual manera sucede con los pagos de servicios sin identificación del ordenante.

Se ha realizado un cuadro de doble entrada donde mostramos las funcionalidades que actualmente se tienen en los principales bancos locales y se señala si la entidad cuenta o no con dicha funcionalidad, para con esto obtener un total y poder comparar.

Tabla 5: Funcionalidades de los ATMs actualmente

Funcionalidad	Nosotros	Banco A	Banco B	Banco C
Retiro	Si	Si	Si	Si
Depósitos	Si	Si	Si	Si
Depósitos (sin identificación)	No	Si	Si	No
Transferencias mismo banco	Si	Si	Si	Si
Transferencias interbancaria	No	Si	No	No
Cambio de clave	Si	Si	Si	Si
Consulta saldos / Mov.	Si	Si	Si	Si
Pago de Servicios	Si	Si	No	No
Pago de Servicios (sin ID)	No	Si	No	No
Adelanto de Sueldo	Si	No	No	Si
Pago de Tarjeta de Crédito	Si	Si	Si	Si
Monedero	No	Si	No	No
Disposición de Efectivo de TC	Si	No	Si	No
Efectivo Móvil	No	No	Si	Si
	9	**11**	**9**	**8**

Fuente: Elaboración propia

Tabla 6: Funcionalidades de los ATMs con biometria mediante huella digital

Funcionalidad	El Banco	Banco A	Banco B	Banco C
Retiro	Si	Si	Si	Si
Depósitos	Si	Si	Si	Si
Depósitos (sin identificación)	Si	Si	Si	No
Transferencias mismo banco	Si	Si	Si	Si
Transferencias interbancaria	Si	Si	No	No
Cambio de clave	Si	Si	Si	Si
Consulta saldos / Mov.	Si	Si	Si	Si
Pago de Servicios	Si	Si	No	No
Pago de Servicios (sin ID)	Si	Si	No	No
Adelanto de Sueldo	Si	No	No	Si
Pago de Tarjeta de Crédito	Si	Si	Si	Si
Monedero	No	Si	No	No
Disp. de Efectivo de TC	Si	No	Si	No
Efectivo Móvil	No	No	Si	Si
	12	**11**	**9**	**8**

Fuente: Elaboración propia

El resultado claramente muestra que antes nuestra entidad se encontraba ocupando el segundo lugar, respecto a funcionalidades, junto al Banco B pero con la biometría sería el que tenga la mayor cantidad.

4.4 Proyección Transaccional – Modelo SARIMA

Se utilizó el programa estadístico EViews para aplicar el modelo. Se cargó la información de la tabla para tener una gráfica que muestre la tendencia.

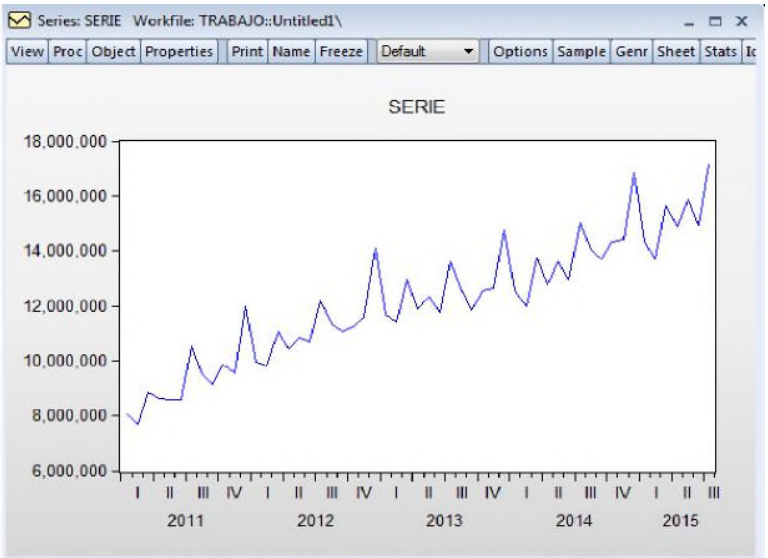
Tabla 7: Histórico de transacciones Canal ATM

mes	2011	2012	2013	2014	2015	2016
ene	8,062,000	9,935,000	11,649,000	12,549,000	14,331,000	
feb	7,706,000	9,804,000	11,398,000	11,984,000	13,701,000	
mar	8,852,000	11,073,000	12,962,000	13,735,000	15,632,000	
abr	8,621,000	10,455,000	11,891,000	12,793,000	14,881,000	
may	8,560,000	10,827,000	12,343,000	13,629,000	15,847,000	
jun	8,588,000	10,693,000	11,755,000	12,943,000	14,924,000	
jul	10,517,000	12,177,000	13,607,000	15,008,000	17,173,000	
ago	9,520,000	11,302,000	12,640,000	14,073,000		
sep	9,161,000	11,056,000	11,825,000	13,692,000		
oct	9,858,000	11,249,000	12,560,000	14,309,000		
nov	9,540,000	11,565,000	12,625,000	14,425,000		
dic	11,963,000	14,082,000	14,740,000	16,843,000		

Fuente: Área de Canales alternativos

Como paso 1 hicimos la evaluación de la tendencia. Se apreció que la serie tiene tendencia creciente.

Figura 11: Evaluación de la tendencia



Fuente: Elaboración propia

Como paso 2 aplicamos el test de raíz unitaria para obtener un valor significativo. Esto se aplica para saber si la serie tiene o no que ser diferenciada (tendencia creciente, no estacionaria en media).

Figura 12: Test de raíz unitaria 1

Null Hypothesis: SERIE has a unit root
Exogenous: Constant
Lag Length: 6 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-0.505005	0.8811
Test critical values:	1% level	-3.574446	
	5% level	-2.923780	
	10% level	-2.599925	

*MacKinnon (1996) one-sided p-values.

Augmented Dickey-Fuller Test Equation
Dependent Variable: D(SERIE)
Method: Least Squares
Date: 11/23/15 Time: 20:24
Sample (adjusted): 2011M08 2015M07
Included observations: 48 after adjustments

SERIE(-1)	-0.031731	0.062833	-0.505005	0.6163
D(SERIE(-1))	-0.926291	0.144582	-6.406669	0.0000
D(SERIE(-2))	-1.168437	0.201094	-5.810405	0.0000
D(SERIE(-3))	-1.037453	0.244295	-4.246728	0.0001
D(SERIE(-4))	-0.881533	0.246685	-3.573915	0.0009
D(SERIE(-5))	-0.350911	0.209106	-1.678150	0.1011
D(SERIE(-6))	-0.526092	0.146207	-3.598273	0.0009
C	1207375.	816313.1	1.479058	0.1470

Fuente: Elaboración propia

Figura 13: Test de raíz unitaria 2

Null Hypothesis: SERIE has a unit root
Exogenous: Constant
Lag Length: 4 (Automatic - based on SIC, maxlag=5)

Augmented Dickey-Fuller test statistic		-0.679797	0.8423
Test critical values:	1% level	-3.568308	
	5% level	-2.921175	
	10% level	-2.598551	

*MacKinnon (1996) one-sided p-values.

Augmented Dickey-Fuller Test Equation
Dependent Variable: D(SERIE)
Method: Least Squares
Date: 11/23/15 Time: 20:33
Sample (adjusted): 2011M06 2015M07
Included observations: 50 after adjustments

SERIE(-1)	-0.044358	0.065252	-0.679797	0.5002
D(SERIE(-1))	-1.108570	0.139171	-7.965503	0.0000
D(SERIE(-2))	-1.127254	0.173282	-6.505318	0.0000
D(SERIE(-3))	-0.884503	0.169898	-5.206087	0.0000
D(SERIE(-4))	-0.527286	0.132729	-3.972650	0.0003
C	1224039.	806097.5	1.518475	0.1360

Fuente: Elaboración propia

Figura 14: Test de raíz unitaria 3

Null Hypothesis: SERIE has a unit root
Exogenous: Constant
Lag Length: 3 (Automatic - based on SIC, maxlag=3)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-0.634034	0.8535
Test critical values:	1% level	-3.565430	
	5% level	-2.919952	
	10% level	-2.597905	

*MacKinnon (1996) one-sided p-values.

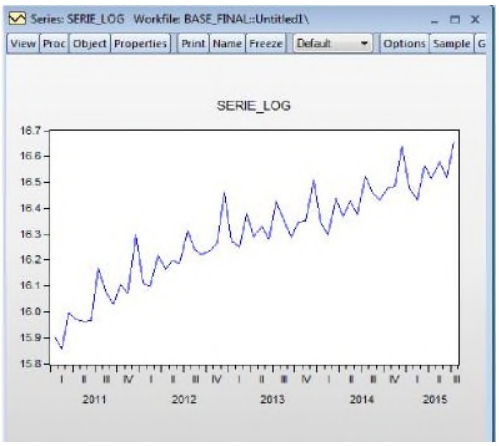
Augmented Dickey-Fuller Test Equation
Dependent Variable: D(SERIE)
Method: Least Squares
Date: 11/23/15 Time: 20:34
Sample (adjusted): 2011M05 2015M07
Included observations: 51 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
SERIE(-1)	-0.045276	0.071409	-0.634034	0.5292
D(SERIE(-1))	-0.903208	0.146012	-6.185864	0.0000
D(SERIE(-2))	-0.735277	0.160067	-4.593567	0.0000
D(SERIE(-3))	-0.413410	0.138516	-2.984563	0.0045
C	1003465.	877407.4	1.143670	0.2587

Fuente: Elaboración propia

De los diversos tests de raíz unitaria aplicados a la serie, se tiene que para ninguna diferenciación es significativo (Prob. < 0.05), por ende se procedió a analizar el logaritmo a la serie.

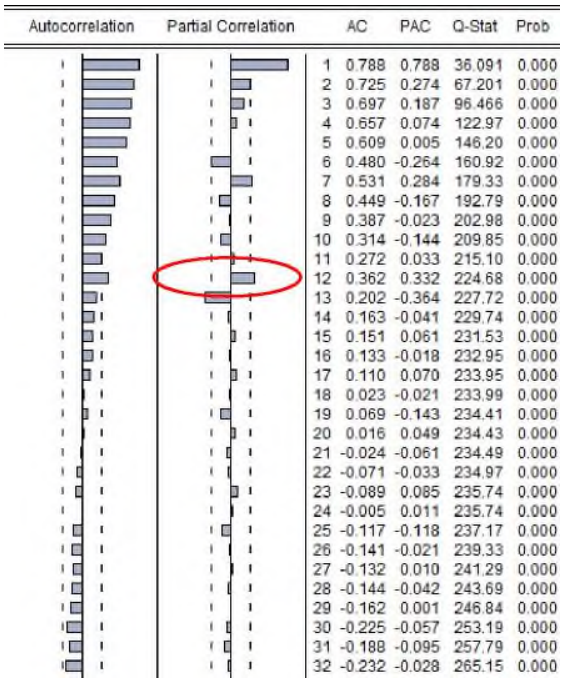
Figura 15: Logaritmo de la serie



Fuente: Elaboración propia

Para nuestro modelo se tiene una tendencia creciente por lo que se diferencia la serie y presenta estación en el rezago 12. Con esta serie trabajaremos.

Figura 16: Correlograma de la serie



	AC	PAC	Q-Stat	Prob
1	0.788	0.788	36.091	0.000
2	0.725	0.274	67.201	0.000
3	0.697	0.187	96.466	0.000
4	0.657	0.074	122.97	0.000
5	0.609	0.005	146.20	0.000
6	0.480	-0.264	160.92	0.000
7	0.531	0.284	179.33	0.000
8	0.449	-0.167	192.79	0.000
9	0.387	-0.023	202.98	0.000
10	0.314	-0.144	209.85	0.000
11	0.272	0.033	215.10	0.000
12	0.362	0.332	224.68	0.000
13	0.202	-0.364	227.72	0.000
14	0.163	-0.041	229.74	0.000
15	0.151	0.061	231.53	0.000
16	0.133	-0.018	232.95	0.000
17	0.110	0.070	233.95	0.000
18	0.023	-0.021	233.99	0.000
19	0.069	-0.143	234.41	0.000
20	0.016	0.049	234.43	0.000
21	-0.024	-0.061	234.49	0.000
22	-0.071	-0.033	234.97	0.000
23	-0.089	0.085	235.74	0.000
24	-0.005	0.011	235.74	0.000
25	-0.117	-0.118	237.17	0.000
26	-0.141	-0.021	239.33	0.000
27	-0.132	0.010	241.29	0.000
28	-0.144	-0.042	243.69	0.000
29	-0.162	0.001	246.84	0.000
30	-0.225	-0.057	253.19	0.000
31	-0.188	-0.095	257.79	0.000
32	-0.232	-0.028	265.15	0.000

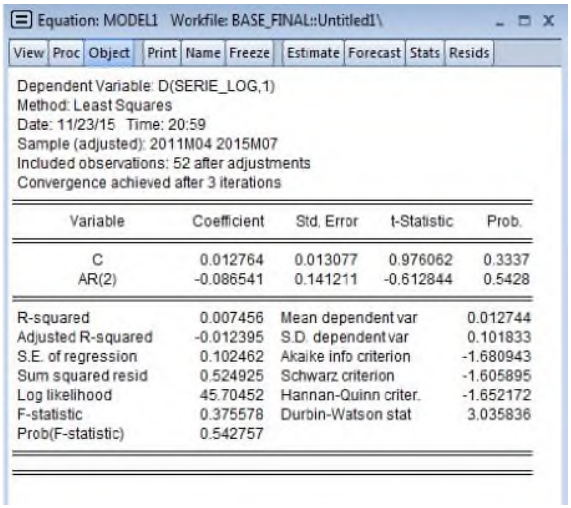
Fuente: Elaboración propia

Del correlograma de los residuos se tiene que las probabilidades son mayores5ϑ

a 0,05 indicando que nuestro modelo es adecuado.

Como paso 3 tomamos un primer modelo AR (2)

Figura 17: Modelo AR (2)



Equation: MODEL1 Workfile: BASE_FINAL::Untitled1\

View | Proc | Object | Print | Name | Freeze | Estimate | Forecast | Stats | Resids

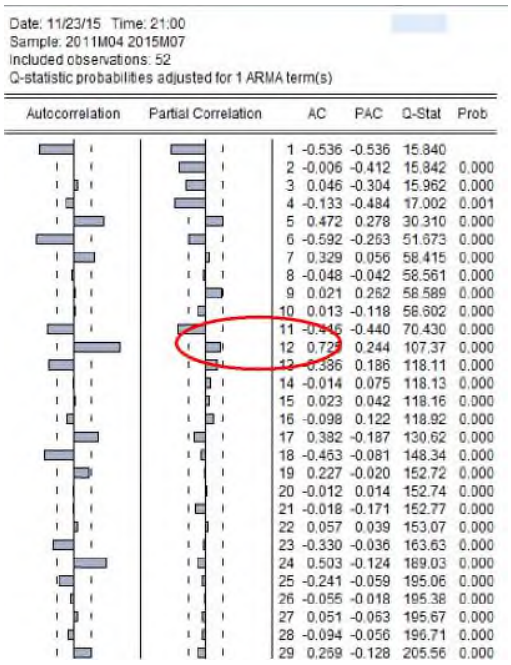
Dependent Variable: D(SERIE_LOG,1)
Method: Least Squares
Date: 11/23/15 Time: 20:59
Sample (adjusted): 2011M04 2015M07
Included observations: 52 after adjustments
Convergence achieved after 3 iterations

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.012764	0.013077	0.976062	0.3337
AR(2)	-0.086541	0.141211	-0.612844	0.5428

R-squared	0.007456	Mean dependent var	0.012744
Adjusted R-squared	-0.012395	S.D. dependent var	0.101833
S.E. of regression	0.102462	Akaike info criterion	-1.680943
Sum squared resid	0.524925	Schwarz criterion	-1.605895
Log likelihood	45.70452	Hannan-Quinn criter.	-1.652172
F-statistic	0.375578	Durbin-Watson stat	3.035836
Prob(F-statistic)	0.542757		

Fuente: Elaboración propia

Figura 18: Correlograma Modelo AR (2)



Date: 11/23/15 Time: 21:00
Sample: 2011M04 2015M07
Included observations: 52
Q-statistic probabilities adjusted for 1 ARMA term(s)

Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	-0.536	-0.536	15.840	
		2	-0.006	-0.412	15.842	0.000
		3	0.046	-0.304	15.962	0.000
		4	-0.133	-0.484	17.002	0.001
		5	0.472	0.278	30.310	0.000
		6	-0.592	-0.263	51.673	0.000
		7	0.329	0.056	58.415	0.000
		8	-0.048	-0.042	58.561	0.000
		9	0.021	0.262	58.589	0.000
		10	0.013	-0.118	58.602	0.000
		11	-0.416	-0.440	70.430	0.000
		12	0.723	0.244	107.37	0.000
		13	-0.386	0.186	118.11	0.000
		14	-0.014	0.075	118.13	0.000
		15	0.023	0.042	118.16	0.000
		16	-0.098	0.122	118.92	0.000
		17	0.382	-0.187	130.62	0.000
		18	-0.453	-0.081	148.34	0.000
		19	0.227	-0.020	152.72	0.000
		20	-0.012	0.014	152.74	0.000
		21	-0.018	-0.171	152.77	0.000
		22	0.057	0.039	153.07	0.000
		23	-0.330	-0.036	163.63	0.000
		24	0.503	-0.124	189.03	0.000
		25	-0.241	-0.059	195.06	0.000
		26	-0.055	-0.018	195.38	0.000
		27	0.051	-0.053	195.67	0.000
		28	-0.094	-0.056	196.71	0.000
		29	0.259	-0.128	205.56	0.000

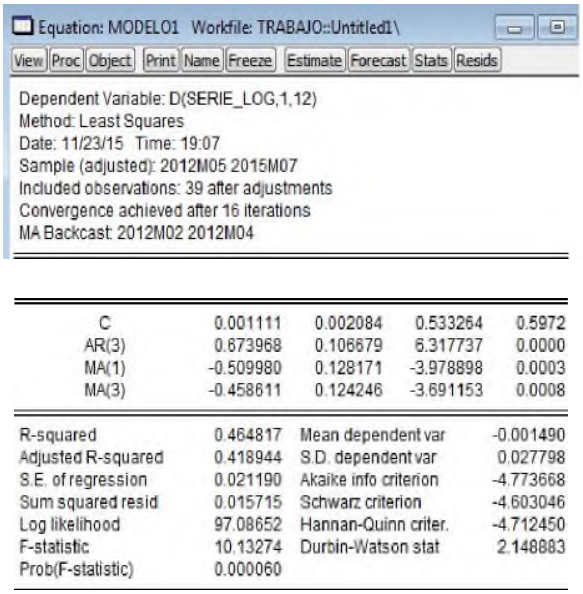
Fuente: Elaboración propia

Analizando los residuos del modelo, tenemos que las probabilidades aun no son mayores a 0,05 por lo tanto nuestro modelo aun no es óptimo.

Del mismo correlograma de residuos se tiene un posible modelo AR (3), MA (1), MA (3) con una posible estacionalidad en "12".

Como paso 4 hallamos otro correlograma y sobre los residuos se tiene que las probabilidades son mayores a 0,05 indicando que nuestro modelo es adecuado.

Figura 19: Validación de probabilidades



Equation: MODEL01 Workfile: TRABAJO::Untitled1\

View | Proc | Object | Print | Name | Freeze | Estimate | Forecast | Stats | Resids

Dependent Variable: D(SERIE_LOG,1,12)
Method: Least Squares
Date: 11/23/15 Time: 19:07
Sample (adjusted): 2012M05 2015M07
Included observations: 39 after adjustments
Convergence achieved after 16 iterations
MA Backcast: 2012M02 2012M04

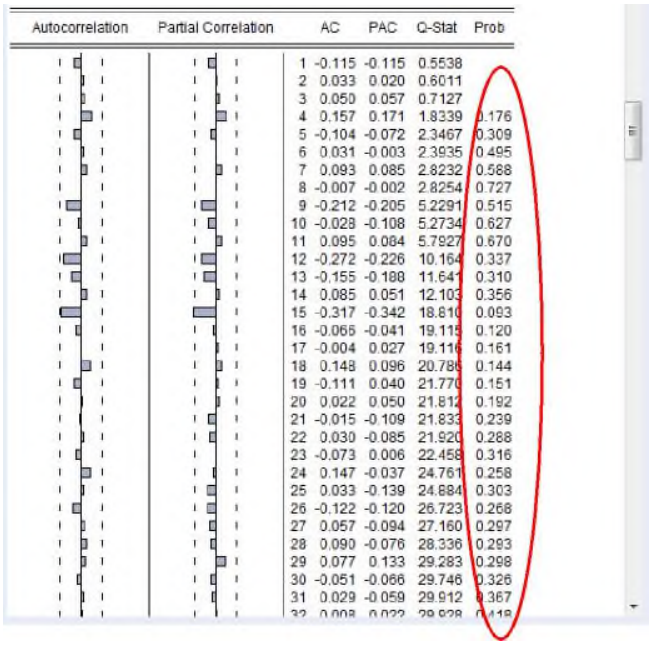
C	0.001111	0.002084	0.533264	0.5972
AR(3)	0.673968	0.106679	6.317737	0.0000
MA(1)	-0.509980	0.128171	-3.978898	0.0003
MA(3)	-0.458611	0.124246	-3.691153	0.0008

R-squared	0.464817	Mean dependent var	-0.001490
Adjusted R-squared	0.418944	S.D. dependent var	0.027798
S.E. of regression	0.021190	Akaike info criterion	-4.773668
Sum squared resid	0.015715	Schwarz criterion	-4.603046
Log likelihood	97.08652	Hannan-Quinn criter.	-4.712450
F-statistic	10.13274	Durbin-Watson stat	2.148883
Prob(F-statistic)	0.000060		

Fuente: Elaboración propia

Respecto al análisis de los correlogramas primero evaluamos los 5 primeros rezagos del AR y los 3 primeros del MA, generalmente es así. Mirar en qué posición va saliendo y siempre comenzar por el menor y luego ir aumentando en cada prueba que se va realizando e ir fijando en los residuos que deben estar todas las barras dentro de la franja. Si no es así ir aumentando las que salen pero siempre de menos a más porque a veces cuando incluyes las menores se corrige las otras mayores que salían de la franja y de esta manera se va armando el modelo.

Figura 20: Correlograma validación de probabilidades



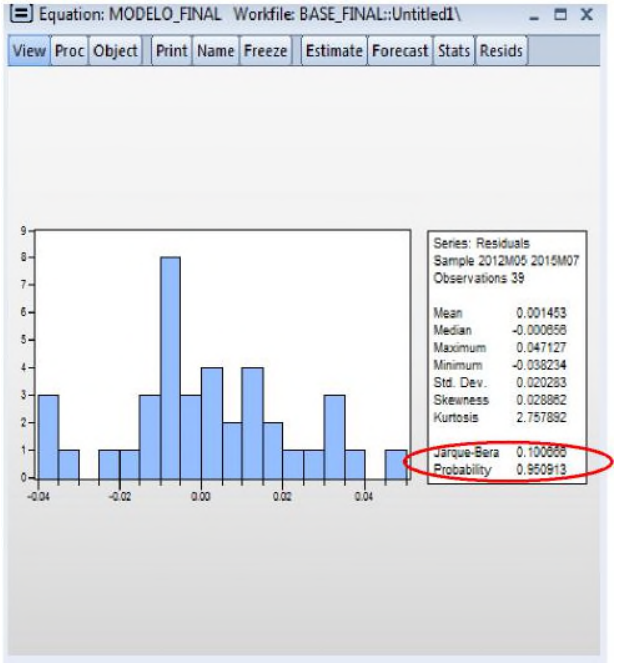
Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	-0.115	-0.115	0.5538	
		2	0.033	0.020	0.6011	
		3	0.050	0.057	0.7127	
		4	0.157	0.171	1.8339	0.176
		5	-0.104	-0.072	2.3467	0.309
		6	0.031	-0.003	2.3935	0.495
		7	0.093	0.085	2.8232	0.588
		8	-0.007	-0.002	2.8254	0.727
		9	-0.212	-0.205	5.2291	0.515
		10	-0.028	-0.108	5.2734	0.627
		11	0.095	0.084	5.7927	0.670
		12	-0.272	-0.226	10.164	0.337
		13	-0.155	-0.188	11.641	0.310
		14	0.085	0.051	12.103	0.356
		15	-0.317	-0.342	18.810	0.093
		16	-0.065	-0.041	19.115	0.120
		17	-0.004	0.027	19.116	0.161
		18	0.148	0.096	20.786	0.144
		19	-0.111	0.040	21.770	0.151
		20	0.022	0.050	21.812	0.192
		21	-0.015	-0.109	21.833	0.239
		22	0.030	-0.085	21.920	0.288
		23	-0.073	0.006	22.458	0.316
		24	0.147	-0.037	24.761	0.258
		25	0.033	-0.139	24.884	0.303
		26	-0.122	-0.120	26.723	0.268
		27	0.057	-0.094	27.160	0.297
		28	0.090	-0.076	28.336	0.293
		29	0.077	0.133	29.283	0.298
		30	-0.051	-0.066	29.746	0.326
		31	0.029	-0.059	29.912	0.367

Fuente: Elaboración propia

.

Como paso 5 procedemos a evaluar la normalidad de los residuos.

Figura 21: Normalidad de los residuos



Fuente: Elaboración propia

Se tiene que la probabilidad es 0.950913 > 0.05, por lo tanto los residuos se distribuyen normalmente.

Del correlograma de los residuos (Figura 28) al cuadrado se tiene que no hay heterocedasticidad en los residuos por lo tanto queda en el modelo anterior que tenemos.

Figura 22: Normalidad de los residuos

		1	-0.303	-0.303	3.8732	
		2	0.006	-0.095	3.8747	
		3	0.030	0.003	3.9143	
		4	0.128	0.155	4.6613	0.031
		5	-0.098	-0.007	5.1096	0.078
		6	-0.030	-0.065	5.1537	0.161
		7	0.079	0.035	5.4651	0.243
		8	-0.037	-0.017	5.5371	0.354
		9	0.038	0.053	5.6128	0.468
		10	-0.109	-0.092	6.2723	0.508
		11	0.129	0.056	7.2162	0.514
		12	0.108	0.193	7.9055	0.544
		13	-0.044	0.067	8.0248	0.626
		14	-0.108	-0.106	8.7690	0.643
		15	0.214	0.114	11.809	0.461
		16	-0.063	0.004	12.087	0.521
		17	-0.075	-0.044	12.496	0.567
		18	-0.082	-0.151	13.010	0.602
		19	0.025	-0.127	13.061	0.668
		20	0.019	0.028	13.092	0.730
		21	-0.162	-0.113	15.432	0.632
		22	0.226	0.186	20.217	0.382
		23	-0.130	-0.053	21.899	0.346
		24	0.068	-0.020	22.385	0.378
		25	-0.130	-0.064	24.328	0.330
		26	0.105	-0.015	25.679	0.316
		27	-0.067	-0.081	26.273	0.339
		28	0.042	0.036	26.535	0.380

Fuente: ElaboraciOn propia

Una vez obtenido el modelo correcto se procede a realizar la proyecciOn ingresando los datos histOricos en el aplicativo EViews. A continuaciOn se presenta una tabla con la proyecciOn de transacciones al siguiente año, es decir de agosto del 2015 a julio del 2016 con informaciOn desde enero del 2011. Entre más historia se tenga (más datos) es mejor.

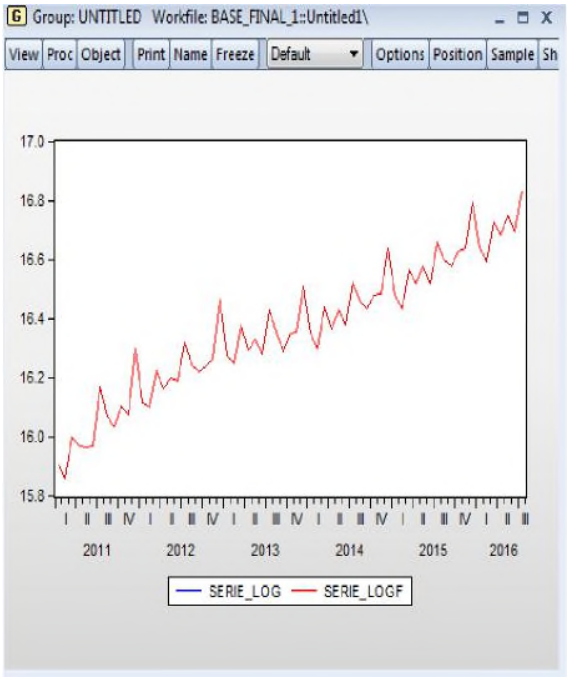
Cabe mencionar que una vez determinado el modelo los datos y meses de la proyecciOn se pueden variar para obtener estimaciones con informaciOn histOrica distinta. Aquí por ejemplo, podríamos decidir que nuestra proyecciOn se alimente con datos de los últimos 2 O 3 años y también si la proyecciOn será del prOximo año (12 meses) o los prOximos 2 años, etc.

Tabla 8: Proyección de transacciones Canal ATM (a julio 2016)

Mes	2011	2012	2013	2014	2015	2016
ene	8,062,000	9,935,000	11,649,000	12,549,000	14,331,000	**16,384,461**
feb	7,706,000	9,804,000	11,398,000	11,984,000	13,701,000	**15,685,285**
mar	8,852,000	11,073,000	12,962,000	13,735,000	15,632,000	**17,873,095**
abr	8,621,000	10,455,000	11,891,000	12,793,000	14,881,000	**17,035,317**
may	8,560,000	10,827,000	12,343,000	13,629,000	15,847,000	**18,164,208**
jun	8,588,000	10,693,000	11,755,000	12,943,000	14,924,000	**17,097,712**
jul	10,517,000	12,177,000	13,607,000	15,008,000	17,173,000	**19,697,697**
ago	9,520,000	11,302,000	12,640,000	14,073,000	**16,129,349**	
sep	9,161,000	11,056,000	11,825,000	13,692,000	**15,627,711**	
oct	9,858,000	11,249,000	12,560,000	14,309,000	**16,354,262**	
nov	9,540,000	11,565,000	12,625,000	14,425,000	**16,510,918**	
dic	11,963,000	14,082,000	14,740,000	16,843,000	**19,231,712**	

Fuente: Elaboración propia

Figura 23: Pronóstico de la serie



Fuente: Elaboración propia

Realizada la proyección con el Modelo Sarima se mostró el incremento transaccional mensual para el 2016 respecto a los años anteriores (señalado en amarillo).

Inicialmente mencionamos que tenemos alrededor de 65.71 millones de transacciones por mes y que de estas el 50% son transacciones de “no clientes”, es decir 32.85 millones de transacciones. De estas el 76% son pagos de servicios, transferencias y pagos varios; es decir que 24.97 millones de transacciones son potencialmente migrables ya que se podrían realizar en los cajeros automáticos.

Así mismo, tenemos alrededor de 14, 985,917 de transacciones totales mensuales que pasan por el canal ATM, que dan una utilidad promedio también mensual de s/. 4, 347,700.

Como meta de área para el 2016, dada por el Área de Planeamiento de Canales, tenemos que lograr migrar el 10% de las transacciones potencialmente migrables que equivalen a 2.49 millones de transacciones por mes.

En la siguiente tabla sumamos las transacciones proyectadas más las transacciones migrables para tener también el pronóstico objetivo. Para fines de este estudio el total de transacciones se está prorrateando igual de manera mensual.

Tabla 9. Proyección de transacciones con migración (a julio 2016)

Mes	Trnsx. Proyec.	Trnsx. Migrables	Total
ene-16	16,384,461	2,490,000	18,874,461
feb-16	15,685,285	2,490,000	18,175,285
mar-16	17,873,095	2,490,000	20,363,095
abr-16	17,035,317	2,490,000	19,525,317
may-16	18,164,208	2,490,000	20,654,208
jun-16	17,097,712	2,490,000	19,587,712
jul-16	19,697,697	2,490,000	22,187,697
ago-15	16,129,349	2,490,000	18,619,349
sep-15	15,627,711	2,490,000	18,117,711
oct-15	16,354,262	2,490,000	18,844,262
nov-15	16,510,918	2,490,000	19,000,918
dic-15	19,231,712	2,490,000	21,721,712
			235,671,727

Fuente: Elaboración propia

Como dato del Área de Planeamiento de Canales tenemos que el costo promedio por transacción en los distintos canales es el siguiente:

- ATM: s/. 0.64
- Agente: s/. 0.49
- Ventanilla: s/. 3.80
- HBK: s/. 0.13

Atender estas 2.49 millones de transacciones por ventanilla equivalen a s/. 9,488,524, atenderlas por cajeros equivalen a s/. 1,598,067. Por lo tanto el ahorro para la Banca Minorista final es de **s/. 7, 890,457**.

4.5 Costos

Para estimar el costo de la implementación consideramos el costo de la instalación del técnico por parte del proveedor Diebold, el costo del lector biométrico, el costo del software SDK y el costo de la licencia.

Los precios han sido obtenidos del proveedor Go IT (2015) y Fulcrum Biometric (2015). El dato de la mano de obra se obtuvo por parte de nuestro proveedor Diebold como información interna del área.

Se muestra el detalle en el siguiente cuadro:

Tabla 10: Costo para implementar lector biométrico

Ítem	Marca	Modelo	Costo	Cantidad	Total
Instalación	Diebold	Mano de obra	$150	233	$34,950
Lector biométric	Lumidigm	V31x	$465	233	$108,345
Software SDK	Verifinger	7.1 Extended	$922	1 (x 233)	$922
Licencia SDK	Verifinger	Fingerprint Matcher	$12	233	$2,742
				Total	**$146,959**

*Valores incluyen IGV

Fuente: Elaboración propia

Del presupuesto total de la Gerencia de Canales Electrónicos el costo más representativo es el que corresponde a la compra de cajeros automáticos (320 equipos a un valor de US$ 15,000 c/u) que es aproximadamente US$ 4,800,000. El costo de implementación de US$ 146,959 equivale al 3.06% del total por lo que la propuesta es completamente viable.

4.6 Intervalos de confianza mediante el Coeficiente V de Aiken

Se utilizó el programa ICaiken para el cálculo de los intervalos de confianza, para darle mayor validez de contenido al estudio. Los datos son ingresados al programa y este calculó automáticamente el rango de valores de las calificaciones (calificación máxima - calificación mínima), el valor del índice V de Aiken, así como los intervalos de confianza en los niveles del 90%, 95% y 99%, niveles comúnmente usados en las estimaciones de intervalos de confianza.

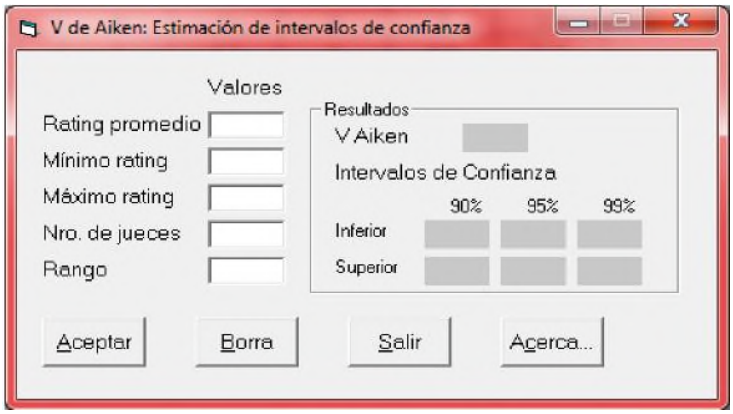
Hemos dividido la investigación en 4 fases y estas son las evaluadas por 6 jueces expertos, con experiencia en la materia y conocimiento del criterio de jueces. Las fases explicadas en el Anexo 4, son las siguientes:

- Fase 1: Viabilidad técnica
- Fase 2: Viabilidad económica
- Fase 3: Viabilidad estratégica
- Fase 4: Diseño (usos) y beneficios

Una vez realizada la evaluación de los jueces ellos proceden a completar el anexo. Se les expuso el objetivo de la validación por fases mediante un formato *ad hoc* e indicó un criterio de calificación del 1 al 5, donde el 1 es el mínimo y 5 el máximo, pudiendo utilizar fracciones. La consideración es a 2 decimales para el valor del promedio.

Esta es la interfaz del aplicativo ICaiken donde hemos colocado nuestros datos para obtener los intervalos de confianza.

Figura 24: Interfaz aplicativo ICaiken



Fuente: Merino,C. & Livia, J

En las siguientes tablas se muestran los valores ingresados según la puntuación dada por los jueces expertos y el cálculo del promedio de estos para poder utilizarlo en el aplicativo. Aquí se enumera cada fase con su detalle.

Tabla 11: Valores obtenidos Fase 1

	Criterio Juez Experto				
Fase 1: Viabilidad técnica	Juez 1	Juez 2	Juez 3	Juez 4	Prom.
Tecnología del parque ATMs	4.5	4	4.5	5	4.50
Características y requisitos DNIe					
Requisitos lector biométrico					

Fuente: Elaboración propia

De la misma manera se procederá a hacer las puntuaciones con el resto de fases. Cada fase tiene un detalle de actividad o sub fase diferente que ha sido revisada por los jueces.

Tabla 12: Valores obtenidos Fase 2

	Criterio Juez Experto				
Fase 2: Viabilidad económica	Juez 1	Juez 2	Juez 3	Juez 4	Prom.
Costos de implementación	4.5	5	4	4.5	4.50
Costos de equipos					
Costos de software					
Costos de licencia					

Fuente: Elaboración propia

Tabla 13: Valores obtenidos Fase 3

	Criterio Juez Experto				
Fase 3: Viabilidad	Juez 1	Juez 2	Juez 3	Juez 4	Prom.
Proyección transaccional	4.5	5	5	4.5	4.75

Fuente: Elaboración propia

Aquí colocamos la última tabla de valores correspondiente a la Fase 4.

Tabla 14: Valores obtenidos Fase 4

	Criterio Juez Experto				
Fase 4: Diseño (usos) y beneficios	Juez 1	Juez 2	Juez 3	Juez 4	Prom.
Adecuación MOC para acceso en los ATMs	4	4.5	4	5	**4.38**
Adecuación de la firma digital					

Fuente: Elaboración propia

La información fue ingresada en el aplicativo ICaiken y se muestra a continuación los valores resultados. Tener en cuenta que se consideró un intervalo de confianza al 95% que es lo más usual. Para el valor del coeficiente de V de Aiken y los intervalos de confianza se están considerando hasta 3 decimales.

Tabla 15: Resultados V de Aiken Fase 1

Promedio		4.50
Valor Min.		1
Valor Max.		5
V de Aiken		0.875
Intervalo de Conf. (95%)	Inf.	0.64
	Sup.	0.96

Fuente: Elaboración propia

El Coeficiente V de Aiken en la Fase 1 es de 0.875 y sus intervalos de confianza son de 0.64 inferior y 0.96 superior, lo que demuestra una alta validez de contenido.

Tabla 16: Resultados V de Aiken Fase 2

Promedio		4.50
Valor Min.		1
Valor Max.		5
V de Aiken		0.875
Intervalo de Conf. (95%)	Inf.	0.64
	Sup.	0.96

Fuente: Elaboración propia

El Coeficiente V de Aiken en la Fase 1 es de 0.875 y sus intervalos de

confianza son de 0.64 inferior y 0.96 superior, lo que demuestra una alta validez de contenido.

Tabla 17: Resultados V de Aiken Fase 3

Promedio		4.75
Valor Min.		1
Valor Max.		5
V de Aiken		0.938
Intervalo de Conf. (95%)	Inf.	0.717
	Sup.	0.989

Fuente: Elaboración propia

El Coeficiente V de Aiken en la Fase 1 es de 0.938 y sus intervalos de confianza son de 0.717 inferior y 0.989 superior, lo que demuestra una alta validez de contenido.

Tabla 18: Resultados V de Aiken Fase 4

Promedio		4.38
Valor Min.		1
Valor Max.		5
V de Aiken		0.845
Intervalo de Conf. (95%)	Inf.	0.606
	Sup.	0.951

Fuente: Elaboración propia

El Coeficiente V de Aiken en la Fase 1 es de 0.845 y sus intervalos de confianza son de 0.606 inferior y 0.951 superior, lo que demuestra una alta validez de contenido.

En resumen se valida que en todas las fases presentadas el nivel de confianza al 95% tiene un valor significativo (valor>0.5) bastante elevado lo que nos lleva a demostrar que el procedimiento elaborado para abarcar los objetivos del estudio de pre factibilidad son es el adecuado.

Tabla 19: Matriz de Riesgos

N°	Riesgo		(Escala) Prob.	(Escala) Impacto	Exposición	Mitigación	Contingencia	Gatillador	Responsable	Estado
	Condición	Consecuencia								
1	Resistencia al cambio	Demora en migración	3	1	3	Apoyo / intervención del JAC	Comunicación a través de la Div. Comercial	Baja transaccionabilidad Reclamos	Administrador Producto	Activo
2	Personal no capacitado	Retraso en la implementación	1	1	1	Capacitaciones	Búsqueda de nuevo personal	Errores reiterativos	Administrador Producto	Activo
3	Migración extrema de “no clientes”	Incomodidad para clientes	1	3	3	Apoyo JAC Derivación	Apoyo Agencia	Saturación	Sub Gerente	Activo
4	Mala estimación transaccional	Colas en ATMs	2	2	4	Apoyo JAC Derivación	Apoyo Agencia	Saturación	Sub Gerente	Activo
5	Productos defectuosos	Reclamos de usuarios	1	1	1	Coordinación con el proveedor	Reunión con proveedor	Fallas constantes	Proveedor	Activo
6	Rotación de personal	Retraso en la implementación	1	1	1	Gestión del conocimiento y documentación	Traspaso de funciones	Problemas en la gestión	Administrador Producto	Activo
7	Robo de lector de huella digital	Inoperatividad biométrica	1	1	1	Coordinación con el proveedor	Reunión con proveedor	Acto delictivo	Proveedor	Activo

Fuente: Elaboración propia

CAPÍTULO V. DISCUSIÓN

Esta investigación tuvo como premisa dar atención a un problema que año tras año seguía afectando a toda la División Comercial y al Área de Canales Alternativos al no poder atender a los “no clientes” en los cajeros automáticos y a su vez lograr una migración a dicho canal. Esto trae consigo un gran ahorro, tanto en la parte operativa como en el aspecto de seguridad por las pérdidas por fraude.

De acuerdo a los resultados mostrados se acepta la hipótesis de presentar una nueva forma de acceso a los servicios de cajeros automáticos implementando lectura biométrica por huella dactilar y sus usos. Esto podrá ser implementado en cualquier institución financiera que tenga problemas similares y busque el ahorro mediante nuevas formas de atención y seguridad pero previamente tendría que hacerse un análisis sobre sus canales con el potencial de transacciones migrables y la tecnología del parque de equipos.

Los bancos que ya han implementado la biometría en cajeros automáticos mediante geometría de mano como el caso de Ogaki Kyoritsu Bank, como indicó Navarrete (2012), obtuvieron un acceso más sencillo y seguro a la red. La ayuda a clientes olvidadizos es también una ventaja ofrecida ya que no es necesario recordar la contraseña. Hay que mencionar que en este caso el cliente necesariamente debe hacer el registro en una agencia del banco antes de poder hacer una transacción en la red de ATMs cosa que no es necesario para los fines de este estudio.

López (2014) indicó que la implementación de biometría en la red de cajeros del Banco Santander brindó seguridad, robustez y eficiencia al negocio. Tanto los clientes como el mismo banco se vieron beneficiados, luego de esto el banco realizó el despliegue en su red completa de oficinas. Con la impresión dactilar no solo se asegura el acceso, si no que garantiza también una única identidad por persona. Como consideración está el enfoque en que dicho banco implementó la biometría ya que su foco puede ser solamente la seguridad o tal vez también la atención de “no clientes” y migración.

Lo curioso de estos casos es que ninguno tiene la particularidad de haber utilizado el documento nacional de identidad como identificación del usuario y utilizar sus propiedades de tarjeta inteligente en el acceso a servicios financieros en los cajeros automáticos. Es una situación sin precedente teniendo en cuenta que el DNI nacional ha sido galardonado durante este año por la Conferencia Latinoamericana de Imprenta de Alta Seguridad como el mejor documento de la región, y que en el país existe una importante red de cajeros automáticos.

A su vez tampoco habrá necesidad de hacer el proceso de registro ya que la información ya viene por defecto en la tarjeta inteligente por lo que el banco solamente es un gestor de esta. No tendremos que realizar toda una campaña o procesos internos para esta fase, esto siempre estará a cargo de la RENIEC.

Por otro lado la proyección transaccional bajo el método estadístico SARIMA apoya a tener resultados periódicos con mayor precisión. La migración transaccional de ventanilla hacia el canal ATM es traducida finalmente en reducción de costos operativos. Sí hay una reducción para la División Comercial, se mostró que los costos de atender una transacción en ventanilla son mucho más altos que el de atender la misma transacción en un cajero automático, por lo que este proyecto está alineado con los objetivos del Área. Efectivamente se apreció un incremento en la proyección del nivel transaccional al canal ATM respecto a los años anteriores.

Más transacciones en el canal no necesariamente implican más ingresos. Al decir esto quiero decir que en general la utilidad del canal depende de un mix transaccional. En el caso todas las transacciones sean retiros definitivamente el canal solamente estaría en pierde ya que el costo de abastecimiento es elevado (puro gasto), pero existen operaciones que tienen comisión como el Adelanto de Sueldo o retiro en otra moneda y eso es lo que da el margen de utilidad.

Por último la reducción de las vulnerabilidades de seguridad del proceso de identificación actual trae consigo menores pérdidas al negocio por fraude bancario y a nivel de competitividad se posesiona a la entidad financiera en primer lugar respecto a las funcionalidades en el canal cajeros automáticos.

El resultado de los intervalos de confianza dan solides a nuestro estudio, tras cumplir con los criterios que jueces expertos consideran obligatorios y al considerar las grandes oportunidades que la aplicación tendría en el negocio y el país.

CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES

6. 1 CONCLUSIONES

Si bien los sistemas biométricos no son perfectos (la tasa de error es mínima, puede presentarse un error en cien mil) consideramos que estos actualmente son la mejor alternativa en el país para lograr una correcta y rápida autenticación, aumentando considerablemente la seguridad.

Esta investigación sólo muestra dos de las varias aplicaciones que tiene la biometría. Se podrían utilizar el resto de sus aplicaciones en otras áreas de la empresa.

Con esta nueva tecnología también podemos lograr la migración transaccional que es uno de los principales objetivos del Área de Canales Alternativos, que trae consigue eficiencia y ahorro de costos operativos. Así mismo, se generan en el proceso oportunidades comerciales.

La información obtenida a través de los métodos estadísticos da fiabilidad al estudio.

Los principales beneficios obtenidos para el Banco son:

- Reducción de riesgo de suplantación y lavado de activos, atención de no clientes fuera de ventanilla
- Menores pérdidas por fraude
- Reducción de tiempos de atención, traducidos en desaturación
- Mejora de imagen corporativa, nueva tecnología
- Ventaja competitiva, descongestión de ventanillas al poder derivar más transacciones a los ATMs
- Match On Card, validación en el punto (ahorro)
-

Y los beneficios para el usuario son:

- Menor riesgo de fraude
- Mayor comodidad y conveniencia -
Reducción de tiempos de espera -
Nuevas funcionalidades
- Inclusión financiera

Cabe mencionar que las marcas y modelos mostrados en este estudio no son los únicos disponibles. En el mercado existe una amplia gama de variedades para utilizar de acuerdo a las necesidades de cada usuario.

Por último mencionar que la innovación tecnológica debe ir acompañada de procesos internos que la soporten, y que el personal este debidamente capacitado para poder llevarlo adelante.

6. 2 RECOMENDACIONES

Las recomendaciones a corto plazo luego de haber realizado este estudio de pre factibilidad son:

- Que el proveedor Diebold inicie pruebas en laboratorio con el lector biométrico Lumidimg en los cajeros automáticos del Banco
- Brindar funcionalidad de pago de servicios con empresas más representativas (empresas top 20)
- Configurar el sistema de los cajeros para soportar una nueva funcionalidad de entrega de duplicado de tarjeta de debito

A largo plazo son:

- El Banco deberá prepararse para apoyar el proceso de difusión y adopción del DNIe
- Desplegar la lectura biométrica de huellas dactilares en el resto de cajeros automáticos del canal y luego hacer el estudio para otros canales (HBK, agente, etc.)
- Adaptar los procesos y arquitectura del Banco para tener una visión 360° del cliente (versus la visión por “producto” actual)
- Lograr una lógica de prospección para identificar “no clientes” con potencial en base a sus transacciones reveladas y así aprovecharla comercialmente
- El software SDK Verifinger también soporta tecnología biométrica de rostro, iris y voz, por lo que da pie a que en un futuro se pueda implementar la biometría de otro tipo en el resto de canales y la información pueda conversar

BIBLIOGRAFÍA

Banco Continental (2015). Cajeros Automáticos. Recuperado de: https://www.bbvacontinental.pe/personas/canales/cajeros-automaticos/

Banco de Crédito del Perú (2015). Cajeros Automáticos. Recuperado de: https://www.viabcp.com/wps/portal/viabcpp/personas/bcp-sin-bcp/producto-bcp-sin-bcp/!ut/p/b1/vZJdj6IwFIZ iz Aoe2AhUsE5UtAoSBwQxAEsSDgBwq fp3NJruz2Zm52cxpc5ImT897-vYwERMw0SnpyyK5ls0pqd7O0SxmbRWu4cZFC4kXgeZbwEDSKwIueALhn8BMd_TEQFQVbMw9Ae8l-el9CzJYJnHAQpItZKOI8f6S-sy6vXT2qOpQg0TI6zTktUQ5biAVhY-jILqZWUaSBUl0vJLo0uRhmj-lpPbRJolW5jrW8KAse0QM9SuNQ5GmeVn5mxNuxu8-j3lYu3PlxATjgzW2PErmIa6NTFbqlmNB6dEidmeCgSV1Bc3UuElmdsUjXznX1P71XvBBiOArv3QmKnf1yz2tX8ALxohHCLOvHITPOZG9L6AKRMJaMuVqxtQRc9NAPw38Cn3QYPgH8cY-YIUwA2Ng9Dq020tE5js6ayM6KyJYOKTRdorqWRwczsyzz7Jvg6BsXsoHm6JsmbW1XIOvMd7y5KPeqER--EETsdwvOvluQ-27B_-H7-aWnbECiyDHcQjzSBAY3wlvDmi3WXRj3UH8bDFUSLtEenK-21LFxuPproXtrnAGxJRBHtK9-PpgLtbSBbL-fmcZytswEUjIcXXlgN1CbaBkIkZlRPqlXZp1Oa0ZgBaO5wPHJH1raH9iAPR9CMdmRPNCnOj85oBSRquh17Z4WyA82If7FLZuJJtZhMGEtt6j3T1l64vRFbv1erDiZAApPNll/dl4/d5/L2dBISEvZ0FBIS9nQSEh/

Bancolombia (2015). Modalidades de Fraude. Recuperado de: http://www.grupobancolombia.com/seguridades/ModalidadesTarjetas.asp?mc=3

BiometricInstitute (2015). AboutBiometrics. Recuperado de: http://www.biometricsinstitute.org/pages/about-biometrics.html

Chávez, N. (junio de 1997) MODELOS ARIMA. Revista y Cultura. Artículos y Estudios. Recuperado de: http://www.scielo.org.bo/scielo.php?pid=S2077-33231997000100005&script=sci arttext

Costa, L. (2007). Prospeccao e implementacao de tecnologia de identificacaobiometrica. Recuperado de: http://es.slideshare.net/IstRio/prospeco-e-implantao-de-tecnologia-de-identificao-biomtrica

Costa, S. (2001). Evolucao dos Métodos de VerificacaoPessoal. Clasificacao e Verificacao de ImpressoesDigitais. (Tesis Profesional). Escola Politécnica da Universidade de Sao Paulo. Recuperado de: http://www.teses.usp.br/teses/disponiveis/3/3140/tde-18032002-102113/en.php

Diario Oficila de la República del Perú El Peruano. Lima. Perú (21 de octubre 2012). Ley N° 27269 "Ley de Firmas y Certificados Digitales". Recuperado de: http://www.reniec.gob.pe/portal/pdf/certificacion/ANEXO10.pdf

Ecured. (2015). Firma Biométrica. Recuperado de: http://www.ecured.cu/index.php/FirmaBiom%C3%A9trica

Editalia. (2015). Firma Biométrica. Recuperado de: http://www.firma-biometrica.com/firma-biometrica

Escurra, L. (1989). Cuantificación de la validez de contenido por criterio de jueces. Revista de Psicología PUCP, Vol. 6 (1- 2), 103-111. Recuperado de: http://revistas.pucp.edu.pe/index.php/psicologia/article/view/4555/4534

FBI. (2015). Recuperado de: https://www.fbi.gov/about-us/cjis/fingerprintsbiometrics/biometric-center-of-excellence/

Ferrero, R. (10 de enero de 2011) ARIMA. Modelos no estacionarios estacionales. Recuperado de: http://statisticalecology-st.blogspot.pe/2009/09/modelos-no-estacionarios.html

FulcrumBiometric (2015). Dispositivos biométricos. Recuperado de: http://es.fulcrumbiometrics.com/el-es-s18f/Escaner-de-huellas-dactilares-multiespectrales-Lumidigm-V-serie-V311

Go IT (2015). Catálogo de productos: Recuperado de: http://www.goit.cl/brochures/VeriFinger SDK Catalogo 2014-04-17.pdf

HandsonBanking (2015). ¿Qué es un cajero automático (ATM)?. Recuperado de: http://handsonbanking.org/htdocs/es/a/ba/atm/

Hernández, A. (s.f.) Propuesta de Estándar para el Uso Seguro de Tecnologías Biométricas. (Proyecto de Tesis). Recuperado de: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/bibliografia.html
Interbank (2015). Cajeros Global Net. Recuperado de: http://www.interbank.com.pe/cajeros-global-net

Interbank comienza pruebas de reconocimiento facial en cajeros automáticos. (diciembre, 2012). Gestión. Recuperado de: http://gestion.pe/tu-dinero/interbank-comienza-pruebas-reconocimiento-facial-cajeros-automaticos-2051329

Internet: canal moderno que facilita las transacciones financieras. (abril, 2015). Con Nuestro Perú.Recuperado de:http://www.connuestroperu.com/economia/46119-internet-canal-moderno-que-facilita-las-transacciones-financieras

KAL (2015). KAL ATM Software. Recuperado de: http://www.kal.com/es/

Klecius, A. (2007). Estudo do uso de biometria para autenticacaoemterminais de auto-atendimento. (Tesis Profesional). UNICEUB - Centro Universitario de Brasilia. Recuperado de: http://repositorio.uniceub.br/bitstream/123456789/3127/2/20168377.pdf

Lima de la Luz, M. (1984). Delitos Electrónicos en Criminalia. México: Porrúa

López, D. & Martínez, C. (21 de mayo de 2013). Modelado de pérdidas en una transmisión de video por medio de series de tiempo ARIMA y SARIMA. Recuperado de:http://www.scielo.org.co/scielo.php?pid=S0123-921X2013000300006&script=sci arttext

López, T. (22 de noviembre 2014). Banco Santander Brasil implanta la biometría. No sólo economía. Recuperado de: http://nosoloeconomia.com/banco-santander-brasil-implanta-la-biometria/

Mission ATM (27 de noviembre de 2013). ¿Cómo funciona un cajero automático? Recuperado de: http://missionatm.com/blog/tag/cajero-automatico/

Mite,J. , Rodríguez, M. & Franco, J. (s.f.). Sistema de Control y Gestión de Personal para PYMES, basado en Sistemas Biométricos. Escuela Superior Politécnica del Litoral - ESPOL. Recuperado de: https://www.dspace.espol.edu.ec/bitstream/123456789/19200/1/ResumenCycit%20Grupo06.pdf

Navarrete, C. (15 de abril 2012). Banco japonés implementará cajeros automáticos biométricos que escaneará la mano del cliente. Biobio Chile. Recuperado de: http://www.biobiochile.cl/2012/04/16/implementan-cajeros-automaticos-biometricos-que-funcionan-escaneando-la-mano.shtml

Parker, D. (1990).Crime by computer.New York: Prentice Hall & IBD

Podkarpacki Banco Cooperativo (2015). Biometría. Recuperado de: https://www.pbsbank.pl/biometria

Radicy, A (16 de abril de 2014). Slideshare. RENIEC / Ayuda memoria DNI electrónico. Recuperado de: http://es.slideshare.net/aradicy/ayuda-memoria-dnie

RENIEC (2012). Documento Nacioanl de Identidad - DNIe. Recuperado de: http://www.reniec.gob.pe/portal/pdf/01dnie.pdf

RENIEC (2013).Estandarización del Upgrade de la solución sistema Automático de Identificación de Impresiones Dactilares (AFIS). Recuperado de: http://www.reniec.gob.pe/Transparencia/intranet/imagenes/noticias/comunicado/INFORME-TECNICO-RS-011-2013-SGEN.pdf

RENIEC (2015). DNI electrónico. Recuperado de: http://portales.reniec.gob.pe/web/dni/dni

RENIEC: Más de 1,200 peruanos cuentan actualmente con DNI electrónico (08 de marzo de 2014). RPP Noticias. Recuperado de: http://rpp.pe/lima/actualidad/reniec-mas-de-1200-peruanos-cuentan-actualmente-con-dni-electronico-noticia-675347

Rojas, G. (2007). Arquitectura de un Sistema Biométrico para Identificación Personal. Recuperado de: https://gjorge.files.wordpress.com/2007/12/afis.jpg

Sánchez, R. (200). Mecanismos de Autenticación Biométrica Mediante Tarjeta Inteligente. (Tesis Doctoral). Universidad Politécnica de Madrid. Recuperado de: http://oa.upm.es/844/1/09200001.pdf

Scotiabank (2015). Cajeros Automáticos. Recuperado de: http://www.scotiabank.com.pe/Acerca-de/servicios-bancarios/cajeros-automaticos

Secretaría (A/Conf.144/5) (27 de agosto 1990). Prevención del Delito y Justicia Penal en El Contexto del Desarrollo: Realidades y Perspectivas de la Cooperación Internacional. Octavo Congreso de las Naciones Unidas Sobre Prevención del Delito y Tratamiento del Delincuente. La Habana.

Sixbell. (2015). Biometría de Voz. Recuperado de: http://www.sixbell.cl/sixbell-corporativo/soluciones/biometria-de-voz

Merino, C. & Livia, J. (junio de 2009). Intervalos de confianza asimétricos para el índice la validez de contenido: Un programa Visual Basic para la V de Aiken. Recuperado de: http://www.um.es/analesps/v25/v251/19-251.pdf

TEKSOL (2015). Biometría multiespectral: Recuperado de: http://www.teksol-ar.com/wp-content/uploads/2014/03/Folleto V-31x esp.pdf

Tellez , J. (1996). Derecho Informático (2 Ed.). México: Mc Graw Hill

Vector ITC Group (2014). Culmina la primera fase de implantación de la solución de Biometría de Vector ITC Group en Banco Santander Brasil. Recuperado de: http://www.vector-itcgroup.com/

Ventas en Seguridad (12 de julio 2012). Implementan lector biométricos en cajeros automáticos en Brasil: Recuperado: http://www.ventasdeseguridad.com/201207066568/noticias/empresas/implementan-lectores-biometricos-en-cajeros-automaticos-en-brasil.html

Vera, M. (10 de noviembre 2014). Biometría Rostro. [Post en Prezi]. Recuperado de: https://prezi.com/qjnbwzulfi9s/biometria-rostro/

Vigliazzi, D. (2006). Biometria: Medidas de Seguranca (2 Ed.). Florianápolis:

VISA (2014). VISA Webinar. Recuperado de: http://usa.visa.com/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf

GLOSARIO

DNIe: Documento nacional de identidad electrónico que acredita de manera presencial no presencial la identidad de su titular, permite la firma digital de documentos electrónicos, y el ejercicio del voto electrónico.

KAL: Software multifabricante para cajeros automáticos de

bancos. ATM: Automated teller machine o maquina de cajero

automático SDK: Software development kit

PIN: Personal identification number

ISO: Organización Internacional de Normalización (International Organization for Standardization)

RENIEC: Registro Nacional de Identificación y Estado Civil

PKI: Infraestructura de Clave Única (Public Key Infrastructure)

ICAO: Organización de Aviación Civil Internacional (International Civil Aviation Organization)

IEC: Comisión Electrotécnica Internacional (International Electrotechnical Commission)

MOC: March On Card

SMS: Short message service o mensaje corto

CPU: Central processing unit

AFIS: Automatic Fingerprint Identification System

RAW: formato en crudo de imágenes

RSA: Rivest, Shamir y Adleman, es un sistema criptográfico

ANEXOS

Anexo 1

Especificaciones técnicas Lector Lumidigm Voyager V31X Series

REQUERIMIENTOS DEL SISTEMA	
Sistema Operativo	Windows 8 / 8 Embebido (32/64 bit) Windows 7 / 7 Embebido (32/64 bit) Windows XP / XP Embebido Linux (Intel 32 bit y 64 bit)
Interfaz	USB 2.0 de alta velocidad (480 Mbps)
Memoria	64 MB de RAM libre

RENDIMIENTO	
Detección de los dedos hasta obtener imagen	700 ms (típico)
Ubicación de los dedos hasta obtener la imagen	de 800 ms - 1 seg (típico)
Ubicación de los dedos hasta obtener la plantilla o el resultado	900 ms - 1,1 seg (típico)
Detección de dedo con vida	Premium
Protección latentes	Incluye
Encriptación	Vídeo cifrado para la protección de la privacidad / reproducción

PLATINA	
Área de captura	Elipse 18mm x 28mm
Material	Vidrio durable, resistente a productos químicos
Recubrimientos	Ninguno
Mecanismos de desgaste	Ninguno

CUMPLIMIENTO DE LOS ESTÁNDARES
FCC / CE Mark FCC Part 15 Clase B / ICES-003 Clase B EN55022, EN55024 Clase B emisiones radiadas
EN 60950-1/A11:2004 de la Unión Europea
IEC / EN 62471 Ed.1
RoHS

SISTEMA DE IMÁGENES	
Resolución	500 dpi
Profundidad	8 bits, 256 escala de grises
Dimensiones	352 x 544 píxeles
Distorsión de campo	<1% sobre el área activa
Contraste MTF	> 0,135 @ 10 ciclos/mm por onda senoidal

IMAGEN / PLANTILLA	
Formato de la imagen	ANSI INCITS 381
Formato de plantillas	ANSI INCITS 378
Extractor / comparador	MINEX certificado
Almacenamiento de Plantillas	Verificación (1:1): ilimitado

REQUISITOS FÍSICOS	
Dimensiones Totales	3.25 "de ancho x 4.00" de largo x 2,35 "de alto 8,3 cm de ancho x 10.2 cm de largo x 6 cm de alto
Temperatura de operación	0 a 60 ° C
Humedad Rango de Imagen funcional Rango de Operación Dispositivo Almacenamiento	 0-100% sin condensación 0-100% de condensación con carcaza IP65 10-95% de humedad relativa sin carcaza 0-95% de humedad relativa sin condensación (a 40° C)
Inmunidad ESD	IEC 61000-4-2 nivel 4 + / -15 kV Aire
Luz ambiental de operación	Hasta 32 K lux (indirecta)
Protección contra ingreso de polvo y agua	IP65 (sólo el área de platina); el paquete V311 es IP64

Fuente: Limtek

Anexo 2

Especificaciones técnicas Lector Morphosmart 300 Series

- A versatile device that carries out **both enrollment and comparison** (1:1 authentication and 1:N identification)
- **Excellent fingerprint capture and processing performance** with the largest single fingerprint optical sensor on the market (23x23mm, 500 dpi, 256 grey levels)
  - Authentication < 0.7 sec[1]
  - Identification < 0.9 sec in 1:1000 mode[1]
  - Top grade solution to register young or elderly people, manual laborers (mining, textile, etc.)
- **Overall performance certified at the highest levels:**
  - FBI PIV IQS (image quality)
  - MINEX compliant algorithms
  - FIPS 201
  - STQC
  - Common Criteria for fingerprint spoof detection (certified by BSI[2])
- **Accurate:** the false acceptance rate (FAR) is configurable down to 10^{-8} - depending on the security requirements - and maintained regardless of number of users in database
- **Guides the user and automatically controls the image quality** during fingerprint capture
- **Large internal database:** standard capacity of 500 users (2 fingerprints each), extendable to 3000 (with MSO IDENTLITE license) or 5000 (with MSO IDENTPLUS license)
- **Multiple template & image formats:**
  - ISO 19794-2, ANSI/INCITS 378, Morpho Proprietary
  - ISO 19794-4, WSQ compressed image
- **Options:**
  - Smartcard reader
  - Fake finger detection (Common Criteria certified)
  - Security features to protect the communication channel between host and device (integrity check, data encryption)

Software packages

- The **MorphoSmart™ SDK** is available to integrate easily the MSO 300 Series into various applications and use its embedded capabilities:
  - Available for Windows, Linux and Android Platforms
  - Includes a BioAPI interface

  NB: Low level protocol (ILV) is also available
- The MSO 300 Series can also be used with **MorphoKit™**, advanced SDK for the capture and processing of fingerprint images, authentication and identification

		MSO 200	MSO 300	MSO 301	MSO 350	MSO 351
Interface		Serial	USB	USB	USB	USB
Internal database		From 500 to 5000 users (with licenses)				
Fake finger detection		-	-	Yes	-	Yes
Smartcard reader		-	-	-	Yes	Yes
Security layer		Optional				
Certifications	FBI PIV IQS	Yes				
	MINEX compliant algorithms	Yes				
	FIPS 201	-	-	-	Yes	-
	Common Criteria by BSI[2]	-	-	Yes	-	-
	STQC	-	Yes	Yes	Yes	Yes

[1] Includes detection, encoding and matching
[2] BSI = Bundesamt für Sicherheit in der Informationstechnik (German Federal Agency for the Security of Information Technologies)

Fuente: Morpho

Anexo 3

Especificaciones técnicas Software Verifinger SDK

Se recomienda el uso de imágenes de **500 dpi** de resolución para VeriFinger. La resolución minima soportada por VeriFinger es de 250 dpi.
Todas las plantillas deben ser cargadas en RAM antes de identificar, por lo tanto el tamaño máximo de la base de datos de plantillas está limitado por la cantidad de RAM disponible.
El algoritmo de comparación y extracción de plantillas biométricas VeriFinger está diseñado para ejecutarse en procesadores multinúcleo permitiendo alcanzar el máximo desempeño posible en el hardware utilizado.

Especificaciones del motor dactilar VeriFinger 7.1				
	Plataforma Android (1)		Plataforma PC (2)	
Componentes de extracción	Embedded Fingerprint Extractor	Embedded Fingerprint Client	Fingerprint Extractor	Fingerprint Client
Tiempo de extracción (seg.)	1.34	1.20	1.34	0.60
Componentes de comparación	Embedded Fingerprint Matcher		Fingerprint Matcher	
Velocidad de comparación (huellas por seg.) (3)	3.000		40.000	
Tamaño de un registro dactilar (bytes)	700 – 6.000 (configurable)			

(1) Requiere ejecutarse en dispositivos Android con procesador SnapDragon S4, Krait 300 (4 núcleos 1,51 Ghz)
(2) Requiere ejecutarse en Pc o portátil con procesador Intel Core 2 Q9400, QuadCore 2.67 Ghz, para alcanzar el desempeño indicado.
(3) Los tiempos están proporcionados bajo el escenario de velocidad maximizada. Las plantillas se deben extraer a partir de imágenes no superiores a 500x500 pixeles. Configurar el algoritmo de comparación para una mayor precisión o usar plantillas a partir de imágenes mas grandes puede requerir un hardware más poderoso para alcanzar la velocidad especificada.

Fuente: Go IT

Anexo 4

Formato de Fases

Cada fase debe ser calificada con un valor del 1 al 5 donde 1 es el mínimo y 5 el máximo. Pueden utilizarse decimales.

Fase 1: Viabilidad técnica — PUNTUACIÓN ( )

- Tecnología del parque de cajeros automáticos - Características y requisitos DNIe
- Requisitos lector biométrico

Fase 2: Viabilidad económica — PUNTUACIÓN ( )

- Costos de implementación
- Costos de equipos - Costos de software - Costos de licencia

Fase 3: Viabilidad estratégica — PUNTUACIÓN ( )

- Proyección transaccional

Fase 4: Diseño (usos) y beneficios — PUNTUACIÓN ( )

- Adecuación de MOC para el acceso en los ATMs - Adecuación de la firma digital

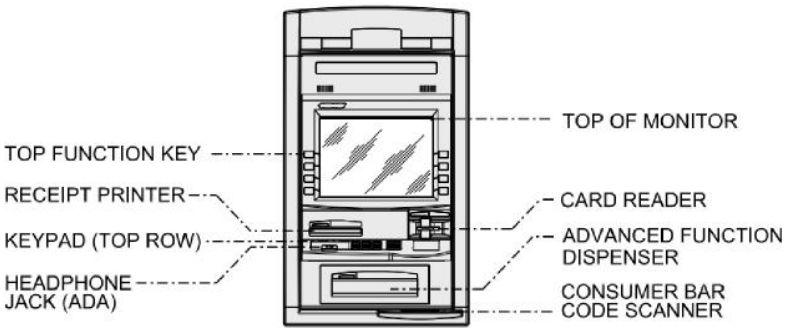
Para el Banco:

- Reducción de riesgo de suplantación y lavado de activos, atención de no clientes fuera de ventanilla
- Reducción de tiempos de atención, traducidos en desaturación
- Mejora de imagen corporativa, nueva tecnología
- Ventaja competitiva: descongestión de ventanillas al poder derivar más transacciones a los ATMs
- Match On Card, validación en el punto

Para el cliente:

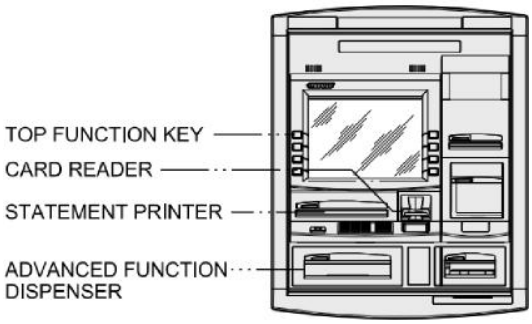
- Menor riesgo de fraude
- Mayor comodidad y conveniencia - Reducción de tiempos de espera - Nuevas funcionalidades
- Inclusión financiera

Figura 25: Partes cajero depósito



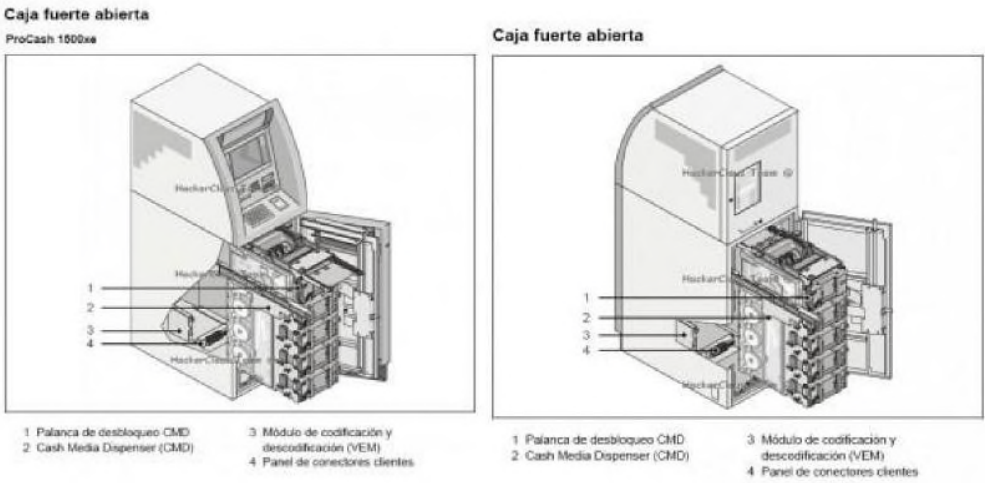
Fuente: Diebold (2015)

Figura 26: Partes cajero multifunción



Fuente: Diebold (2015)

Figura 27: Bóveda cajero lobby frontal

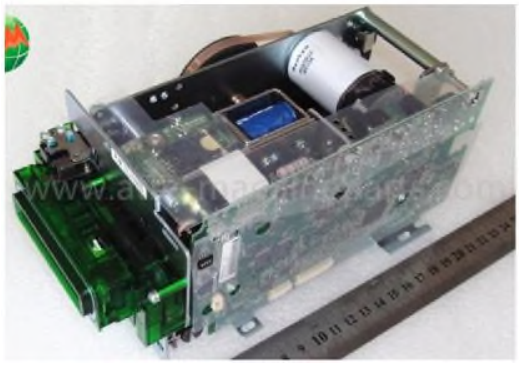


Fuente: Diebold (2015)

Figura 28: Dispensador

Fuente: Fujitsu (2015)

Figura 29: Lector de tarjeta inteligente e impresora



Fuente: Machine Parts (2015)

Figura 30: Lonchera

Fuente: Diebold (2015)

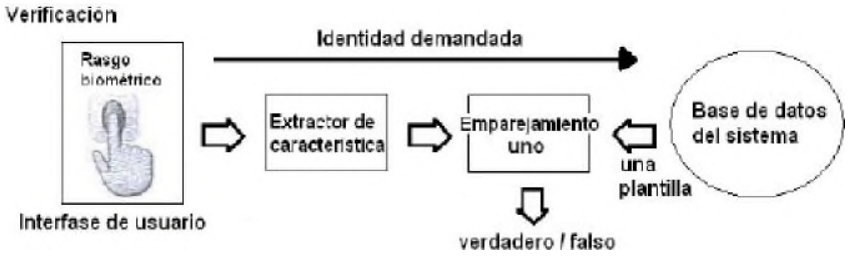
Figura 31: Evolución de los métodos de verificación personal

Fuente: Costa (2015, p.16)

Figura 32: Registro

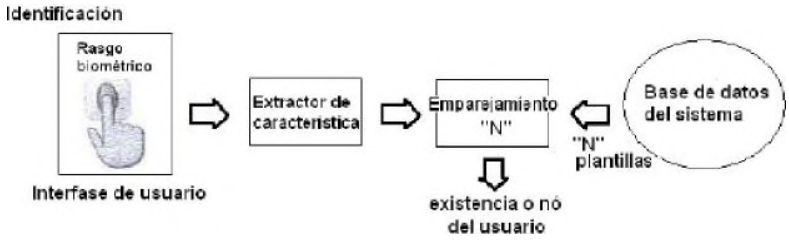
Fuente: Balmelli (2006)

Figura 33: Verificación (1:1)



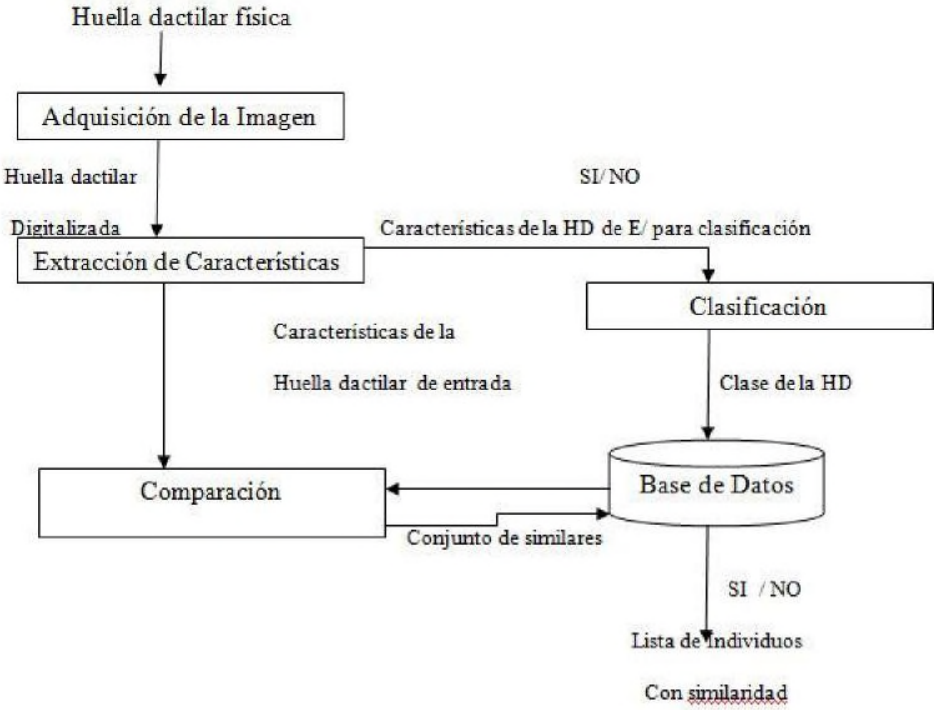
Fuente: Balmelli (2006)

Figura 34: Identificación (1:N)



Fuente: Balmelli (2006)

Figura 35: Diagrama de bloques de un sistema AFIS



Fuente: Rojas, G. (2007)

Figura 36: Características Documento Nacional de Identidad Electrónico

El Documento Nacional de Identidad Electrónico **(DNIe)** es de policarbonato, un material rígido durable con resistencia al calor, al doblado y a los rayos ultravioleta.

El **(DNIe)** contiene un chip criptográfico con certificación Common Criteria EAL5 y sistema Operativo que implementa las especificaciones JavaCard 2.2.2 y Global Platform 2.1.1. Almacena en su memoria datos del ciudadano en formato OACI, certificados digitales y datos biométrico. El chip y el sistema operativo cuentan con la certificación FIPS 140-2 nivel 3.

Medidas:

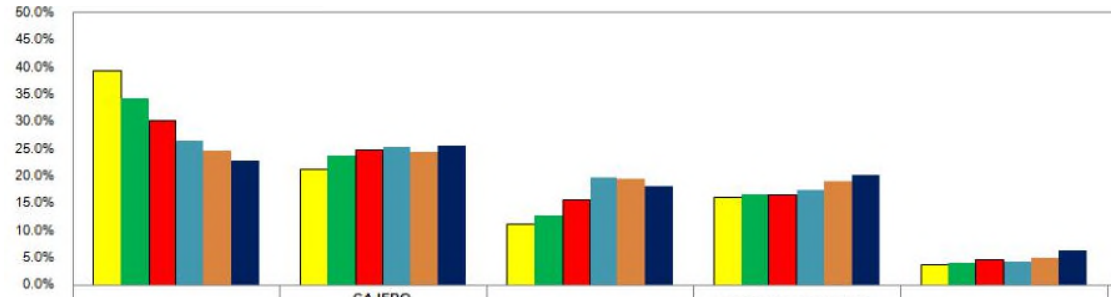
- Ancho: Mínimo 53,92 mm - Máximo 54.18 mm
- Largo: Mínimo 85,47 mm - Máximo 85.90 mm
- Radio de redondeo de esquinas: Mínimo: 2,88 mm - Máximo: 3,48 mm
- Espesor: Mínimo de 0,68 mm - Máximo de 0,84 mm

Fuente: RENIEC (2012)

Figura 37: Elementos de Seguridad del DNIe

Fuente: RENIEC (2012)

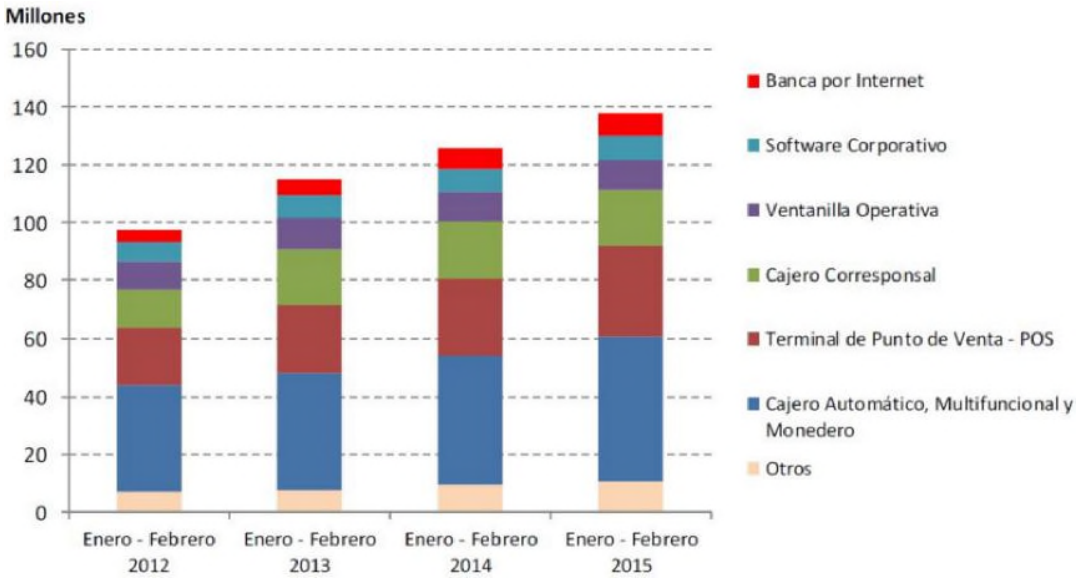
Gráfico 2: Transacciones monetarias por canal de atención: I Trimestre 2010-2015



	VENTANILLA	CAJERO AUTOMATICO, MONEDERO Y MULTIFUNCIONAL	CAJERO CORRESPONSAL	TERMINAL PUNTO DE VENTA (POS)	BANCA POR INTERNET
2010 - I	39.4%	21.2%	11.1%	16.0%	3.6%
2011- I	34.1%	23.7%	12.5%	16.7%	4.1%
2012- I	30.2%	24.7%	15.6%	16.5%	4.5%
2013 - I	26.5%	25.3%	19.8%	17.4%	4.3%
2014 - I	24.6%	24.3%	19.5%	19.1%	5.0%
2015 - I	22.7%	25.6%	18.1%	20.1%	6.4%

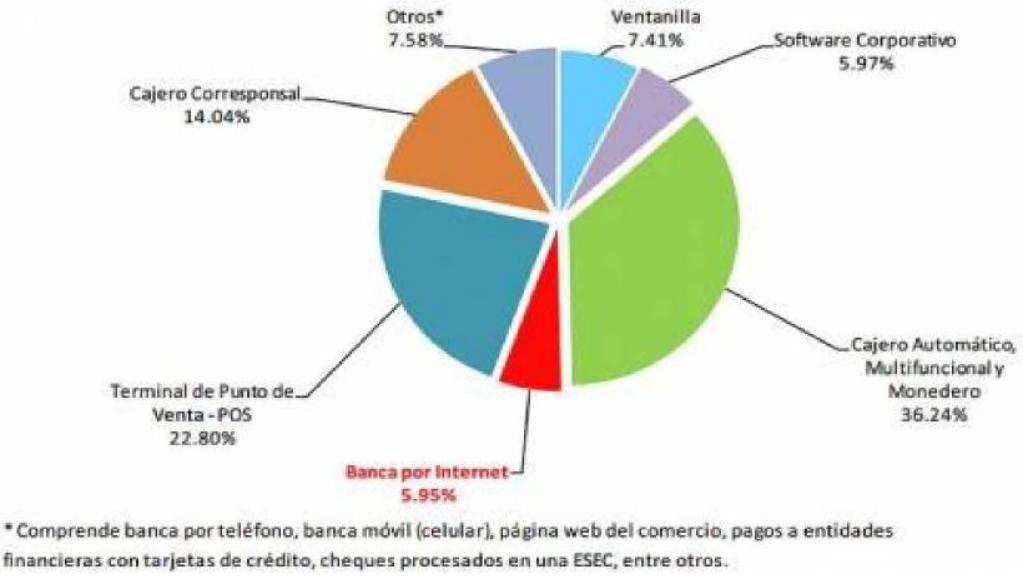
Fuente: ASBANC (2015)

Gráfico 3: Transacciones bancarias con instrumentos distintos al efectivo por canal de atención



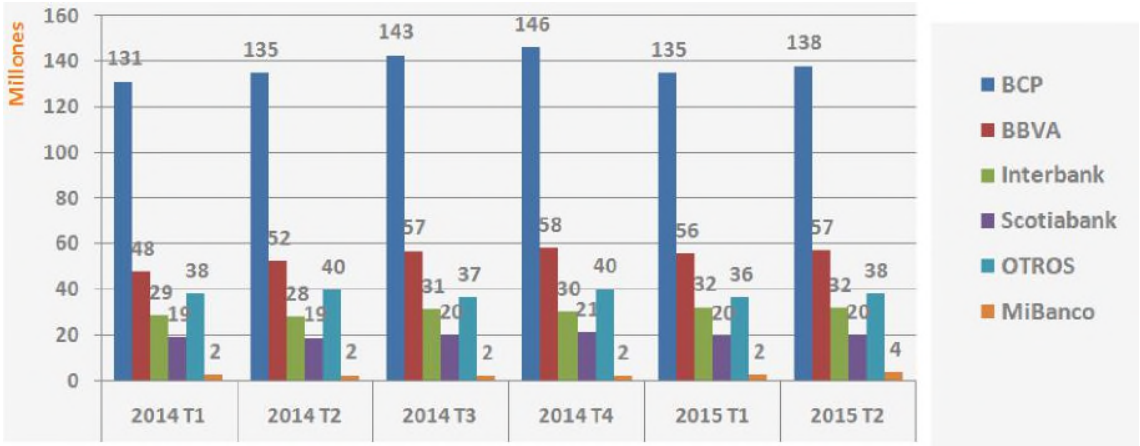
Fuente: ASBANC (2015)

Gráfico 4: Distribución del N de Trans. con instrumentos distintos al efectivo por canal de atención (enero-febrero 2015)



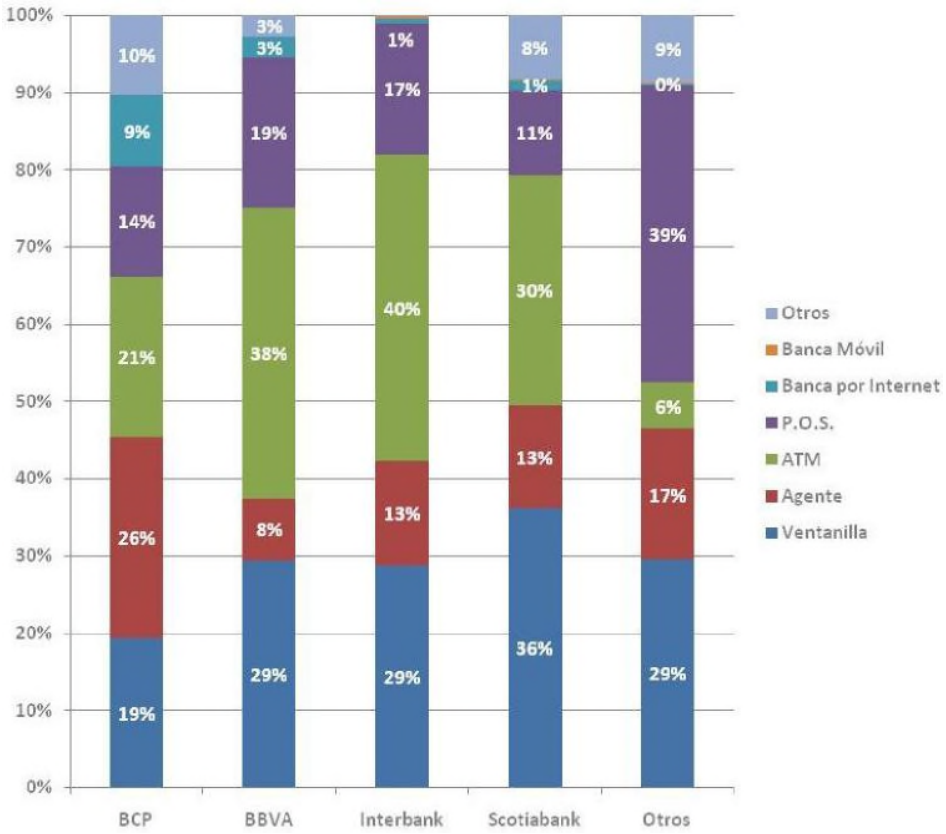
Fuente: ASBANC (2015)

Gráfico 5: Transacciones Monetarias Totales



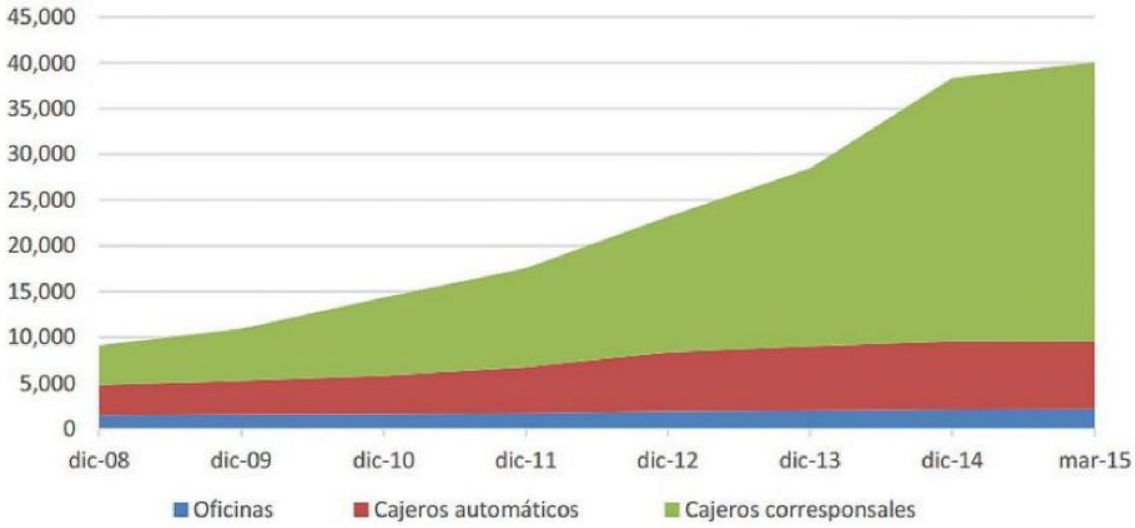
Fuente: ASBANC (2015)

Gráfico 6: Transacciones Monetarias por Canal



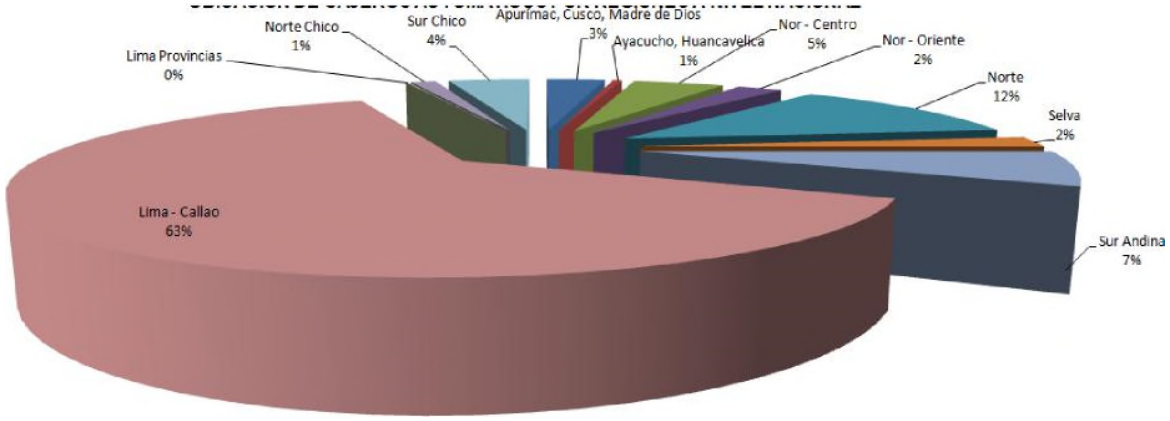
Fuente: ASBANC (ene – jul 2015)

Gráfico 7: Evolución de oficinas, ATMs y agentes (diciembre 08 - marzo 15)



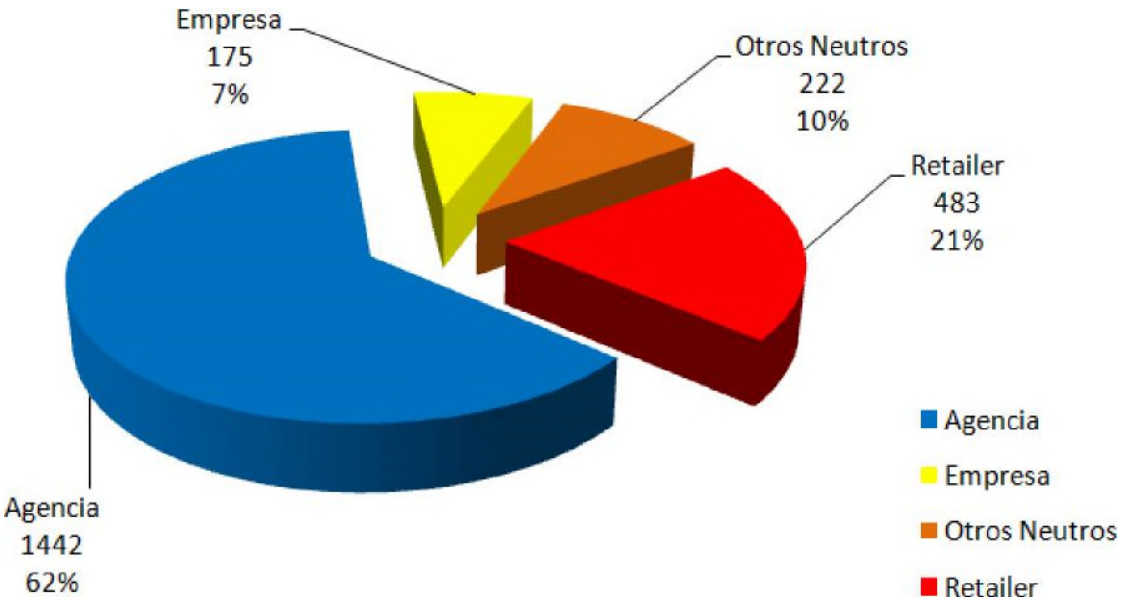
Fuente: ASBANC (2015)

Gráfico 8: Ubicación de ATMS por regiones a nivel nacional (julio a 2015)



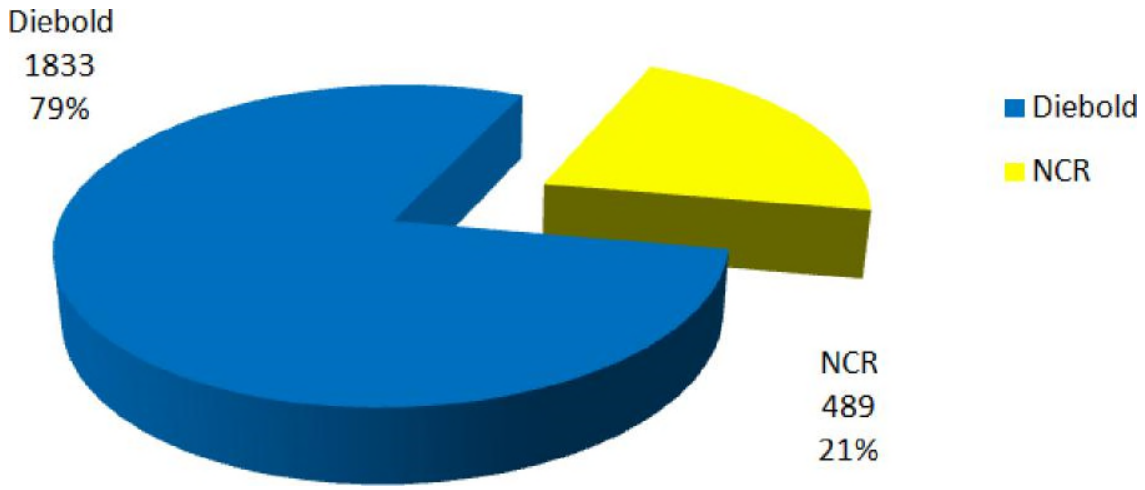
Fuente: ASBANC (2015)

Gráfico 9: ATMs por ubicación (entidad financiera)



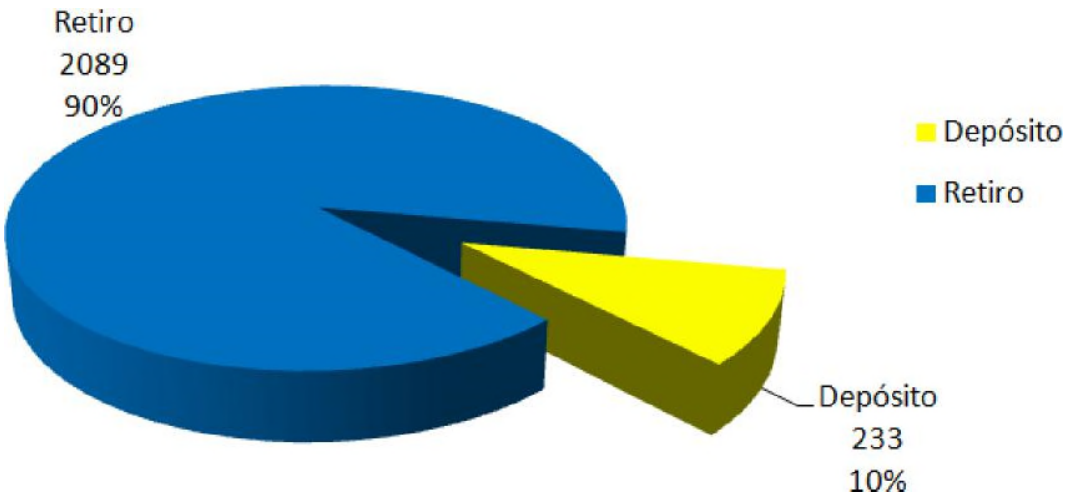
Fuente: Canales Alternativos (2015)

Gráfico 10: ATMs por marca (entidad financiera)



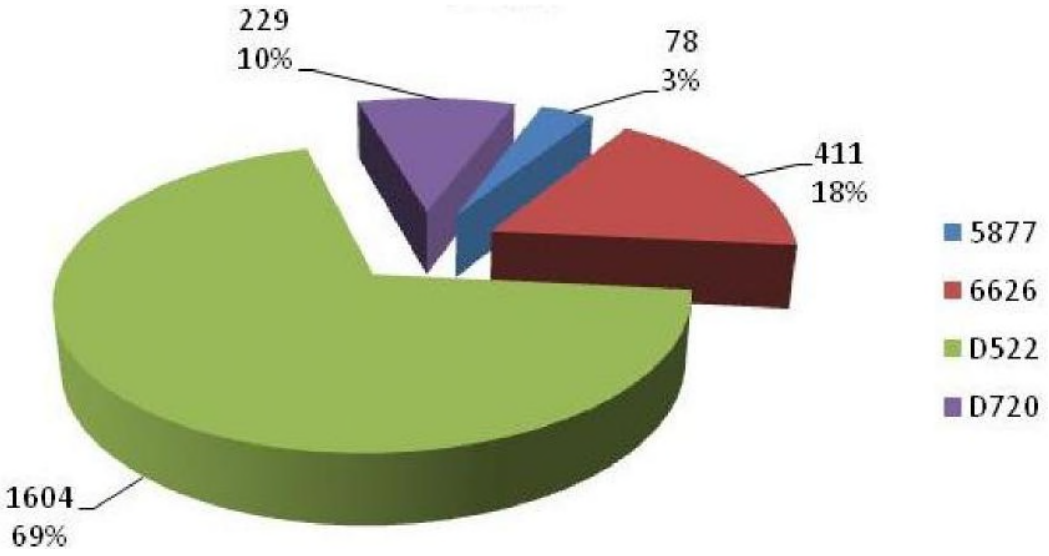
Fuente: Canales Alternativos (2015)

Gráfico 11: ATMs por tipo (entidad financiera)



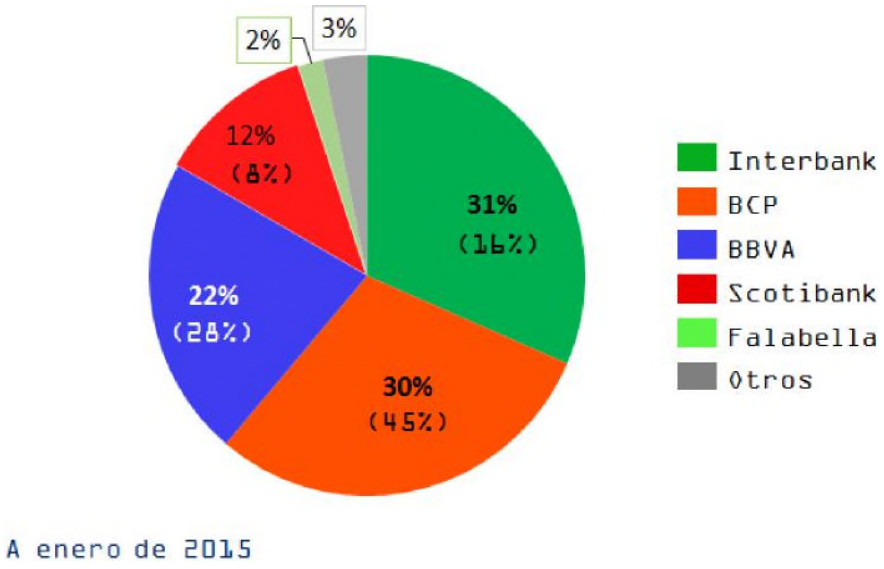
Fuente: Canales Alternativos (2015)

Gráfico 12: ATMs por familia (entidad financiera)



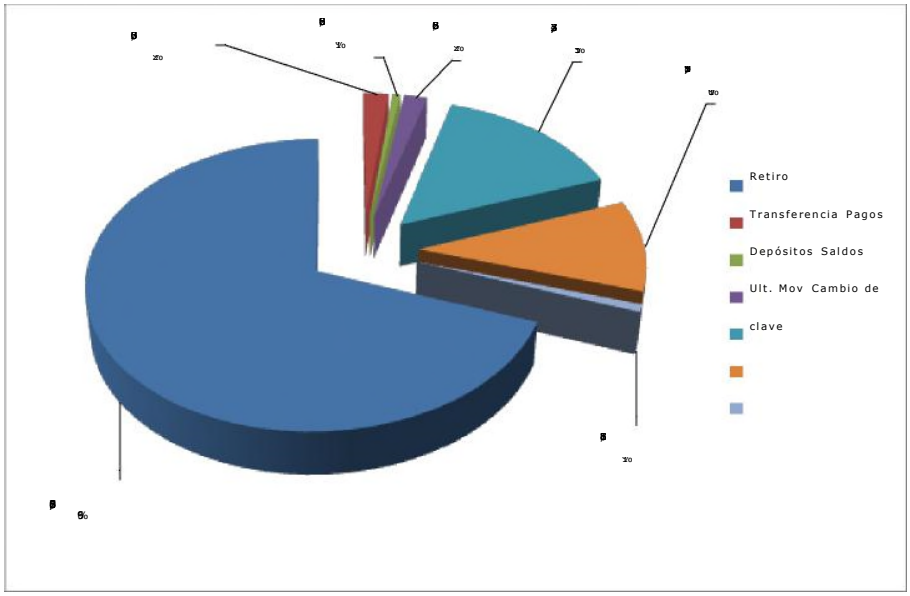
Fuente: Canales Alternativos (2015)

Gráfico 13: Participación de Mercado Transacciones/ N°ATMs



Fuente: Canales Alternativos (2015)

Gráfico 14: Número de transacciones por tipo (promedio a julio 2015)



Fuente: Canales Alternativos (2015)