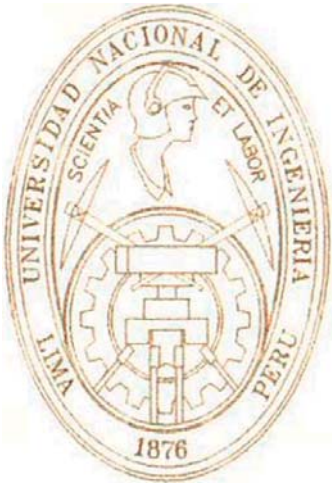
Universidad Nacional de Ingeniería

Facultad de Ingeniería Industrial y de Sistemas



Medios de Pagos - Seguridad en su Producción y uso por Internet para una Institución Bancaria

Informe de Suficiencia

Para Optar el Título Profesional de:

INGENIERO DE SISTEMAS

CARLOS BENIGNO MONTAÑO RIVERA

Lima Perú

2002

Dedicatoria

A la memoria de

mi hermano Cesar.

A Benigno y Noema, mis padres

por su constante motivación.

A Martha, mi esposa por su comprensión y apoyo.

A Omar y Johan, mis hijos por su pronta realización

como una nueva generación de profesionales.

Agradecimiento

Mi más sincera gratitud a los docentes y autoridades de la Facultad de Ingeniería Industrial y de Sistemas, en especial a los profesores del Tercer Programa de Titulación por Actualización de Conocimientos al brindar su dedicación y apoyo en acceder a la obtención del titulo profesional mediante este informe.

INDICE

I. DESCRIPTORES TEMÁTICOS

Comercio electrónico

Sistemas de Pago

Cadena de Valor

Tarjeta de Crédito y Débito

Transacción electrónica virtual

Seguridad

II. RESUMEN EJECUTIVO

El banco es una institución que viene emitiendo tarjetas de uso electrónico que son reconocidas a nivel nacional y mundial, también se usa en transacciones financieras en la tienda virtual (site) del Banco y en comercios tradicionales como medio de pago.

Una tienda virtual es aquella que ofrece productos y servicios a través de la red de internet.

En los sitios de compras por internet y convencional, los medios de pago a utilizar deben estar afiliados a una entidad de marca y prestigio como son Visa, Mastercard, American Express, Dinners, entre otros, las cuales utilizan los estandares internacionales de validación de las tarjetas y del poseedor de la misma para concretar alguna compra en la actualidad.

Las transacciones electrónicas en cajeros y compras en comercios convencionales o virtuales siempre se solicita datos convencionales o el código secreto entregado al tarjeta habiente (cliente del Banco) como información necesaria para la identificación y validación del poseedor de la tarjeta. Por ello realizar alguna transacción financiera en la tienda virtual que posee el banco requiere de una confirmación de autenticación del cliente, para ello se utiliza el código secreto que el banco le entrego, siendo este mismo código secreto el usado en todos los puntos de atención electrónica.

La generación de tarjetas electrónicas que emite el banco están basadas en un esquema de seguridad que utiliza claves maestras que son almacenadas y validadas utilizando software.

El Banco al apreciar esta realidad en sus clientes y con la finalidad de brindar una mayor seguridad es que decide implementar un sistema de generación de tarjetas utilizando un modulo de seguridad conocido como HSM (Host Security Module) tecnología de última generación.

Así mismo también se decide implementar que toda transacción financiera que se realice en la tienda virtual del banco debe hacer uso de un nuevo código secreto de identificación del cliente. Las características de este nuevo código de identificación utiliza técnicas de E-security, lo cual reduce el nivel de riesgo y lo independiza del código utilizada en otros canales convencionales como son Cajeros, Banca Telefónica, Puntos de Venta y en ventanillas de la red de agencias que tiene el banco.

La introducción de este nuevo sistema de seguridad tiene un énfasis estratégico, comercial y tecnológico con el apoyo de los procesos actuales estandarizados que maneja la institución.

Mercado Objetivo

- Todos las personas naturales clientes que tienen tarjetas de débito y crédito del Banco.
- Todas las personas jurídicas clientes que tienen tarjetas de débito y crédito del Banco.

Resumen Comercial

- La tarjeta puede ser obtenida al acercarse el cliente a cualquier oficina del Banco con su documento de identidad.
- El cliente que posea una cuenta de ahorros o cuenta corriente puede obtener una tarjeta de débito sin costo de afiliación.
- Una tarjeta de crédito es obtenida luego de previa evaluación del cliente.
- El cliente puede utilizar su tarjeta en las ventanillas de las agencias del banco, en Cajeros Automáticos, en la banca telefónica, en la banca virtual (Site en Internet) y comercios convencionales o virtuales que estén afiliados a una marca de manejo de tarjetas.
- El cliente al hacer uso de su tarjeta en los diversos medios electrónicos debe ingresar su código secreto, por ello la importancia de su confidencialidad ya que su uso implica firmar electrónicamente toda operación financiera que hagan con ella y no debe ser conocida por otra persona que su propietario.

III. INTRODUCCIÓN

3.1. OBJETIVOS

La seguridad es una constante preocupación que tienen los clientes y emisores de tarjetas de uso electrónico, los clientes deben mantener en absoluta confidencialidad su código secreto en los diferentes canales electrónicos donde la usa y las instituciones financieras deben garantizar la seguridad en su validación y emisión.

A continuación se presenta el desarrollo de un esquema funcional y tecnológico de un sistema de seguridad que permita la generación de códigos secretos de las tarjetas de débito y crédito en forma segura con el propósito de lograr los siguientes estratégicos objetivos:

- Ofrecer tarjetas como instrumentos seguros en los diversos canales electrónicos donde se permite su uso.
- Motivar al cliente al uso del medio electrónico internet, en especial en el site del banco.
- Afianzar el liderazgo en el mercado con los productos y servicios que ofrece la Institución.
- Fidelizar a los actuales clientes y ofrecer a los nuevos instrumentos seguros para transaccionar.

- Cumplir con las normas de seguridad que exigen los patrocinadores internacionales de tarjetas.
- Incrementar el número de transacciones financieras en el site que tiene la institución.

3.2. ALCANCE

Presentar el impacto de la seguridad de la información como solución sobre la cadena de valor de la institución bancaria en la promoción de las transacciones financieras virtuales como estrategia adoptada.

3.3. LOGROS Y LIMITACIONES

Con la implantación de este esquema de seguridad y acceso se fortalece a la institución bancaria en su compromiso establecido de incentivar e incrementar los negocios electrónicos por internet.

Aprendizaje de nuevos esquemas de seguridad en el proceso de generación de tarjetas que permitan garantizar la calidad de las mismas como fuerza de ventas para su colocación en el mercado nacional.

Limitaciones en cuanto a la poca aceptación por el publico en general de realizar negocios y transacciones financieras en forma virtual.

IV. ANTECEDENTES

4.1. DIAGNOSTICO ESTRATÉGICO

La Institución Bancaria es una empresa líder en el Sector Financiero con más de cien años de vida institucional.

A inicios del primer año del nuevo siglo se incursiona en Internet a través de su propio portal de negocios donde se centraliza la oferta de productos y servicios existentes y donde se oferta según convenio la publicación de productos con otros comercios.

El acceso a la Internet en el mercado nacional esta evolucionando paulatinamente a través de cabinas publicas y en forma domestica.

Por el lado de la competencia se están disponiendo a incursionar también en los negocios virtuales con la implementación de sus propios portales en Internet.

4.1.1. FORTALEZAS

El banco tiene un alto volumen y sólido mercado de clientes.

Propicia entre su personal ofrecer una alta calidad de servicio, siendo sus productos y principalmente sus tarjetas de Crédito y Débito reconocidas a

nivel nacional e internacional, para lo cual esta afiliada a marcas como son Visa Internacional y American Express.

Cuenta con su propia y amplia red de Cajeros Automáticos.

Tiene una vasta red de sucursales y oficinas que le permite atender a sus clientes a nivel nacional y subsidiarias en varios países como son Bolivia, Colombia, Panamá y Estados Unidos.

La institución realiza en forma constante la inversión en Tecnología de la Información (hardware y software) de última generación en su área de sistemas, a razón de ello tiene implementado su propio portal en la web.

4.1.2. DEBILIDADES

En su proceso de generación de tarjetas y en su autenticación se utiliza técnicas de implementadas de hace una década, que en la actualidad no cumplen con los procedimientos de seguridad que recomienda Visa Internacional.

4.1.3. OPORTUNIDADES

Las divisiones de Banca Personal y Banca de Servicio de acuerdo a las recomendaciones del área de Seguridad de Información del Banco y Visa Internacional, ven oportuno generar un requerimiento que permita garantizar a los clientes una absoluta confianza en los procedimientos de impresión de códigos secretos.

Además ven conveniente a los actuales clientes que usan su portal el ofrecerles una forma segura de generar un código secreto en línea, nuevo código de mayor longitud, seguro e independiente del código usado en otros medios electrónicos.

Esto permitirá a la institución ofrecer transacciones financieras como es Transferencias a Terceros.

4.1.4. RIESGOS

El banco viene usando hace buen tiempo unas llaves de seguridad para la generación y validación de tarjetas, las mismas que se encuentran registradas en el software usado para este fin, pero el riesgo que existe es la posible exposición de esas llaves de seguridad, esto a razón que los programas fuentes para este fin las registra como una constante.

La institución ve también como un riesgo que los clientes que ingresan a su portal y realizan transacciones financieras utilizan el mismo código secreto para confirmar dichas operaciones que el código que utilizan en otros medios electrónicos como son cajeros automáticos, puntos de ventas en comercios y ventanillas de la red de oficinas del Banco. Este riesgo es cuantificable por el posible incremento de reclamos que recibiría el Servicio de Atención al Cliente.

El nivel de fraudes que tiene el banco en la actualidad es bajo con respecto al volumen de movimiento de transacciones financieras que tiene la

institución, pero esto se puede incrementar por los riesgos indicados anteriormente.

Es de conocimiento del Banco que existe un incremento del fraude a nivel internacional y en especial en nuestra región esto porque existen bandas de delincuentes dedicadas a efectuar ataques a una instituciones con bajo nivel se seguridad.

4.2. DIAGNOSTICO FUNCIONAL

4.2.1. PRODUCTOS

Tarjeta de Crédito Clásica para personas de nivel socioeconómico C, con aproximadamente 200.000 tarjetas emitidas.

Tarjeta de Crédito Oro para personas de nivel socioeconómico A, B y C, se emiten aproximadamente 130.000 unidades

Tarjeta de Débito Clásica para todo tipo de personas, con una emisión aproximada de 1.500.000 unidades.

Tarjeta de Débito Empresarial para negocios de todo nivel, emisión de aproximadamente 20.000 unidades.

4.2.2. CLIENTES

Personas naturales de nivel socioeconómico A, B, C

Negocios de la pequeña, mediana y grandes empresas

4.2.3. PROVEEDORES

Dos proveedores locales de suministro de plásticos para emisión de tarjetas de débito y crédito

Un proveedor local de suministros de formularios y sobres para emisión de tarjetas

Dos proveedores de las marcas internacionales (Visa y American Express) bajo las cuales se emiten las tarjetas, estos proveedores también establecen procedimientos internacionales que norman la generación, seguridad, uso e intercambio financiero a nivel internacional.

Se tiene un proveedor local denominado adquiriente (Visanet) que administra todos los comercios en donde se aceptan las tarjetas como medio de pago.

Se tiene un representante local de la compañía DataCard proveedora del hardware y mantenimiento del equipo DataCard 9000, hardware con el cual se emboza, magnetiza y ensobra las tarjetas.

La compañía RACAL tiene también un representante nacional que ofrece el hardware de seguridad, así mismo este representante ofrece software de seguridad.

4.2.4. PROCESOS

De los diversos procesos que tiene el banco para el desarrollo de sus actividades se detallan a continuación los principales que tienen relación con las tarjetas de Crédito y Débito, estos son:

- Proceso de Generación y custodia de Llaves de Seguridad.

- Proceso de Generación de Claves y su uso en los canales electrónicos.
- Proceso de atención a Clientes en plataforma de agencia.
- Proceso de emisión y reposición de tarjetas de crédito y débito.
- Proceso de atención a clientes en ventanilla de agencia.
- Proceso de atención a clientes en cajeros automáticos.
- Proceso de atención a clientes en puntos de ventas en comercios a nivel nacional e internacional.
- Proceso de atención a clientes en página web.

Estos procesos son descritos a continuación:

4.2.4.1. Proceso de Generación y custodia de Llaves de Seguridad.

Este es el principal proceso mediante el cual se basa toda la seguridad de los medios de pagos como son las tarjetas de Crédito y Débito, la administración de las componentes para generar las diversas llaves que se usan en la generación de las tarjetas, validación y esquemas de seguridad en los todos los canales electrónicos que el banco autoriza su uso.

Este proceso comprende primero la elección de tres custodios para los componentes de la llave principal del banco, para ello se designa a tres funcionarios de alta jerarquía en la institución, ellos deben hacer recepción y custodiar de cada uno de los componentes que envía el patrocinador internacional de las tarjetas, estos componentes permiten generar la llave de control de zona ZCMK (Zone Control Master Key).

Cabe indicar que estos componentes son también administrados, almacenados y custodiados por 3 representantes del patrocinador de las tarjetas, en nuestro caso Visa o American Express.

Los componentes una vez ingresados en el software seguridad de llaves que usa la institución son guardadas en sobres lacrados con su respectiva identificación en las cajas de seguridad que designa el área de Auditoria Interna.

4.2.4.2. Proceso de Generación de Claves y su uso en los canales electrónicos.

Obtenida la ZCMK el área encargada de la seguridad de la información en el Banco procede ingresar en el software de seguridad cada una las llaves que se utilizaran en los otros procesos de generación, transporte y validación de los datos de seguridad que se usan en los medios de pagos como son las tarjetas de crédito y débito, todas estas llaves están almacenas en forma encriptada bajo la ZCMK.

Las principales llaves utilizadas son las siguientes:

- IWK Issuer Working Key, llave principal del emisor de tarjetas con la cual se envía información encriptar al patrocinador de la marca.
- AWK Acquirer Working Key, llave con la cual los adquirientes de medios electrónicos envían información encriptada al patrocinador de las tarjetas.

- PVK Personal Value Key, llave utilizada en el proceso de generación de códigos secretos o PIN (Personal Verification Value) y PVV (Personal Verification Value) dato complementario al PIN que se usa en el proceso de validación del poseedor de la tarjeta.
- CVK Card Verification Value llave usada en la generación del valor de verificación de las tarjetas conocido como CVV (Card Verification Value) dato que es grabado en la banda magnética.
- TWK Terminal Working Key, llaves de trabajo que utiliza el banco en cada uno de los canales electrónicos donde se usan las tarjetas de crédito y débito, estas llaves permiten encriptar la información que es enviada al computador central para su validación.

4.2.4.2. Proceso de atención a Clientes en plataforma de agencia.

Las plataformas es uno de los puntos de atención que tiene el banco, en él se ofrecen a las personas naturales y jurídicas los diversos productos y servicios que tiene la institución.

Cuando una persona desea obtener una tarjeta de crédito se ingresan sus datos generales al sistema para la respectiva evaluación, esta solicitud debe ir acompañada de la fotocopia del documento de identidad y sustentación de ingresos.

También se permite el aperturar cuentas corrientes o de ahorros, en este caso la plataforma hace entrega de una tarjeta de débito con la cual el cliente podrá identificarse como cliente del banco y efectuar transacciones financieras en los distintos canales de atención que ofrece la red del banco.

Cuando un cliente necesita reemplazar su tarjeta ya sea por haber sido extraviada, deteriorada, retenida en algún cajero automático o se le ha olvidado su código secreto se apersona también a este punto de atención para su reemplazo inmediato en caso que sea tarjeta de débito y en el caso de las tarjetas de crédito se tramita la emisión de una nueva.

4.2.4.3. Proceso de emisión y reposición de tarjetas de crédito y débito.

A la aprobación de la solicitud de una tarjeta de crédito de un cliente el software de evaluación crediticia genera la información respectiva que es recibida por el aplicativo de Tarjeta de Crédito que procede a inscribir al cliente en sus respectivas bases de datos y prepara la data que será enviada a la unidad de producción de tarjetas.

En forma similar el software que administra las tarjetas de débito genera la data a ser remitida a la unidad de producción de tarjetas, pero es importante indicar que está información generada no es solicitud de un cliente sino de acuerdo al consumo de tarjetas que experimente cada agencia o sucursal del banco a nivel nacional.

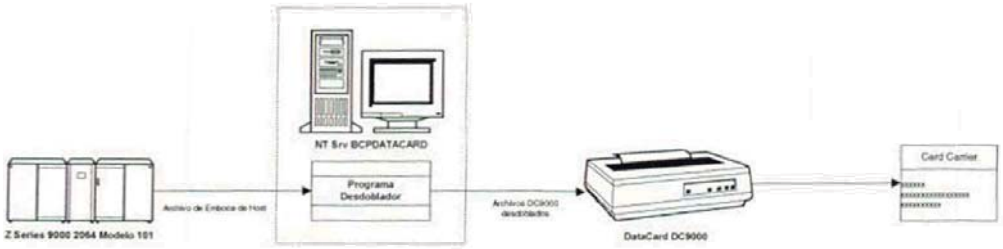
La información remitida por los aplicativos de Tarjeta de Crédito y Tarjeta de Débito es recepcionada electrónicamente por la Data Card 9000

(DC9000), equipo especializado en la producción de tarjetas, que realiza las siguientes fases:

- Embozar: graba el número de la tarjeta en alto relieve, fase que se usa en las tarjetas de crédito.
- Termoimpresión: graba el número de la tarjeta en bajo relieve, las tarjetas de débito usan esta fase.
- Magnetización: graba datos de seguridad en la banda magnética de la tarjeta.
- Impresión de Card Carrier: imprime el número de la tarjeta y código secreto en el card carrier (hoja o formato de bienvenida donde se pega la tarjeta), anteriormente se utilizaba el PINMAILER (sobre de seguridad que contiene el PIN o código secreto) impreso en forma separada que era entregada al cliente en forma independiente de la tarjeta.
- Pegado y Doblado de sobre: Se pega la tarjeta en el card carrier ocultando el código secreto ya impreso, luego se procede a su doblado.
- Ensobrado y sellado: el card carrier es introducido en un sobre y luego este es sellado y embolsado para su distribución.

Se adjunta diagrama del proceso actual de emisión de tarjetas.

ESQUEMA ACTUAL DE PRODUCCIÓN DE TARJETAS - DATACARD



4.2.4.4. Proceso de atención a clientes en ventanilla de agencia.

En todas las ventanillas de la red de agencias y sucursales del banco todo cliente puede efectuar transacciones financieras utilizando su respectiva tarjeta de crédito o débito, como parte de la transacción esta la identificación del poseedor de la tarjeta, para lo cual el cliente debe ingresar su código secreto en los PinPAD (dispositivo electrónico para el ingreso de PIN o código secreto), el dato ingresado es encriptado en este dispositivo y remitido a través de la red hasta el computador central para su validación. Confirmada su autenticidad se tramita la operación que el cliente desea realizar y en caso contrario es rechazada la operación.

4.2.4.5. Proceso de atención a clientes en cajeros automáticos.

Los clientes pueden efectuar una serie de operaciones financieras y de consulta a sus cuentas en la red de cajeros automáticos que tiene el banco,

para ello el cliente debe ingresar su tarjeta y código secreto, de ser conforme el código ingresado el cajero automático le mostrará diversas opciones como son:

- Retiro en efectivo.
- Transferencias entre sus propias cuentas.
- Transferencias a cuentas de terceros o interbancarias.
- Pagos de Servicios.
- Consultas.
- Cambio de Clave.

Cabe indicar que el banco tiene implementado la obligatoriedad de cambio de código secreto a la primera transacción que el cliente realice en un cajero.

4.2.4.6. Proceso de atención a clientes en puntos de ventas en comercios a nivel nacional e internacional.

Los clientes que poseen las tarjetas de crédito y débito del banco pueden efectuar consumos en los diversos comercios afiliados, pero es conveniente indicar que el proceso de atención con tarjeta difiere del tipo de tarjeta.

Con una tarjeta de crédito el comercio esta obligado a solicitar la presentación de algún documento de identidad que permita identificar al poseedor de la tarjeta, también se debe solicitar al cliente que firme el voucher o comprobante del pago.

En cambio con una tarjeta de débito es obligatorio que el cliente ingrese su código secreto en los PINPAD que tiene los puntos de ventas, esto garantiza

al comercio que el poseedor de la tarjeta sea identificado por el banco al validar dicho código.

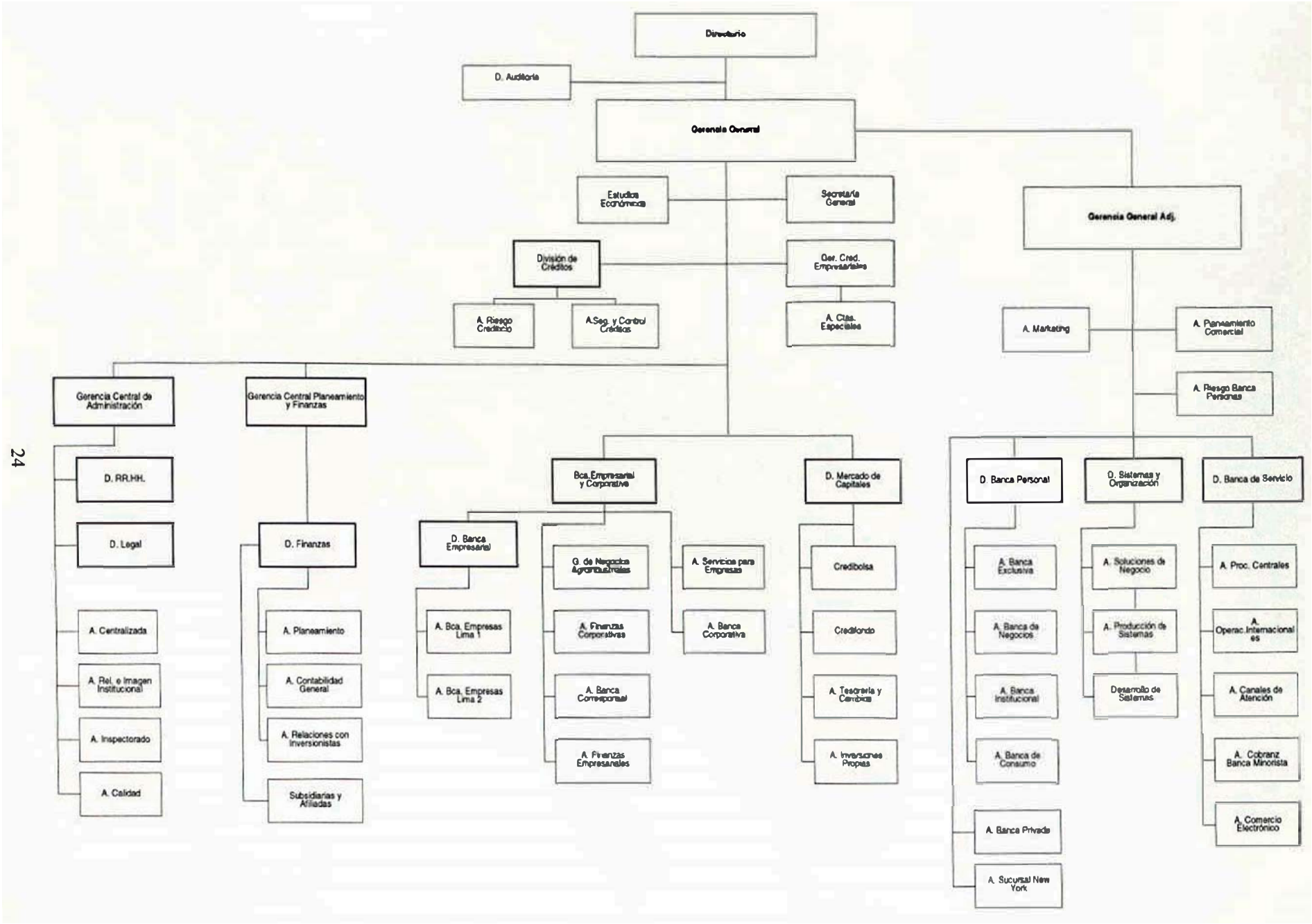
4.2.4.7. Proceso de atención a clientes en página web.

El banco tiene su propia pagina web donde permite a sus clientes realizar una serie de operaciones financieras y de consulta, las principales operaciones financieras son:

- Transferencias entre sus cuentas.
- Transferencias a cuentas de terceros
- Ordenes de pago (giros)
- Pagos a empresas

También se permite consulta de saldos y últimos movimientos de sus cuentas.

4.2.5. ORGANIZACIÓN DE LA INSTITUCIÓN


Directorio
D. Auditoría
Gerencia General
Estudios Económicos
Secretaría General
División de Créditos
Ger. Cred. Empresariales
A. Riesgo Crediticio
A.Seg. y Control Créditos
A. Ctas. Especiales
Gerencia General Adj.
A. Marketing
A. Planeamiento Comercial
A. Riesgo Banca Personas
Gerencia Central de Administración
Gerencia Central Planeamiento y Finanzas
D. RR.HH.
D. Legal
A. Centralizada
A. Rel. e Imagen Institucional
A. Inspectorado
A. Calidad
D. Finanzas
A. Planeamiento
A. Contabilidad General
A. Relaciones con Inversionistas
Subsidiarias y Afiliadas
Bca.Empresarial y Corporativa
D. Mercado de Capitales
D. Banca Empresarial
G. de Negocios Agroindustriales
A. Servicios para Empresas
A. Bca. Empresas Lima 1
A. Bca. Empresas Lima 2
A. Finanzas Corporativas
A. Banca Corporativa
A. Banca Corresponsal
A. Finanzas Empresariales
Credibolsa
Credifondo
A. Tesorería y Cambios
A. Inversiones Propias
D. Banca Personal
D. Sistemas y Organización
D. Banca de Servicio
A. Banca Exclusiva
A. Banca de Negocios
A. Banca Institucional
A. Banca de Consumo
A. Banca Privada
A. Sucursal New York
A. Soluciones de Negocio
A. Producción de Sistemas
Desarrollo de Sistemas
A. Proc. Centrales
A. Operac.Internacionales
A. Canales de Atención
A. Cobranz Banca Minorista
A. Comercio Electrónico

Las unidades que participan en los procesos actuales de manejo de tarjetas bancarias se detallan a continuación:

Unidad de Logística

Encargado de coordinar con los proveedores la adquisición de los insumos y deberá efectuar el envío a sus respectivos centros de consumo. Entre los insumos tenemos:

- Plástico – Tarjeta
- Sobres de entrega
- Encartes de presentación de la tarjeta y/o promociones
- Formato de contrato por afiliación a la tarjeta

Unidad de Producción de Tarjetas

- Realizar el proceso físico de grabación del plástico
- Realizar la distribución de tarjetas a oficinas a nivel nacional
- Administrar los parámetros logísticos para cada oficina de atención a nivel nacional

Unidad de Atención a clientes

- Brindar solución a solicitudes de reclamos de clientes
- Supervisar las transacciones financieras y administrativas de clientes

Unidad de Comercio Electrónico

- Encargado de definir las categorías de comercios electrónicos
- Realizar convenios con comercios electrónicos locales y del exterior
- Afiliar comercios en el portal de intemet del Banco

V. MARCO TEÓRICO

5.1. MARCO CONCEPTUAL DEL COMERCIO ELECTRÓNICO

El comercio electrónico consiste en el intercambio de bienes o servicios realizado mediante la utilización de un flujo electrónico diseñado para facilitar la entrega de los mismos incluido el dinero, a través de los distintos procesos de negocios de las organizaciones.

El avance tecnológico en el área de informática inter-empresarial y de las comunicaciones globales crea una gran demanda de información y de nuevos canales de comercialización. Esto abarca tanto a las organizaciones como a los consumidores. Las organizaciones comienzan a darse cuenta de los beneficios de las tecnologías globales aplicadas a la entrega de nuevos servicios para sus clientes. Esta información interactiva distribuye beneficios a ambos, organizaciones y consumidores y al mismo tiempo define el futuro flujo de información de los negocios.

La tendencia es cada vez mas clara. Los consumidores prefieren los productos fáciles de operar, seguras y prácticos, en vez que del estatus o la apariencia de los bienes o servicios.

Las Instituciones financieras serán intermediarios en la medida en que el consumidor no pueda ir a alguno de los sites a los que desea porque no ha

cerrado trato con alguna institución que direccione el flujo de dinero que intervendrá en la compra.

Comercio Electrónico es un concepto general que engloba cualquier forma de transacción comercial o de negocios que se transmite electrónicamente usando las redes de telecomunicación y utilizando como moneda de cambio el dinero electrónico.

Este intercambio de bienes, servicios e información electrónica. Incluye también las actividades de promoción y publicidad de productos y servicios, campañas de imagen de las empresas, marketing en general, facilitación de los contactos entre los agentes de comercio, soporte post-venta, seguimiento e investigación de mercados, concursos electrónicos y soporte para compartir negocios.

Esta es una perspectiva muy simple, ello implica que el Comercio Electrónico puede entenderse como la automatización mediante procesos electrónicos de los intercambios de información, así como de transacciones, conocimientos, bienes y servicios que en última instancia pueden conllevar o no la existencia de una contraprestación financiera, a través de un medio de pago como son las tarjetas de débito y crédito.

Así, un agente que realiza Comercio Electrónico se basa en un perfil híbrido del rol hasta ahora realizado por cuatro agentes:

- Comercio, que ofrece el bien, servicio o información (se incluye a los bancos).
- Entidad Financiera, que ofrece un medio de pago.
- Operador Logístico, que entrega el producto o mercancía.

- Operadora de Telecomunicaciones, que ofrece la red de comunicaciones.

En tomo a estas cuatro funciones emergen otras dos nuevas funciones que complementan y amplían el escenario de la nueva actividad empresarial:

- Proveedor de Servicio, que es a quien el cliente lo percibe como proveedor del acceso legal telemático a la información, independientemente del propietario de la infraestructura de comunicaciones.
- Intermediario o " Infomediario ", que agrega contenidos de otros proveedores y los comercializa electrónicamente bajo su nombre e imagen al cliente final.

Por ello el Comercio Electrónico se caracteriza por la existencia de tres capas complementarias entre sí:

- Capa Logística, o de intercambio físico de los productos, se basa en la integración de las cadenas logísticas de aprovisionamiento y distribución.
- Capa Transaccional, que posibilita el intercambio de información, a través de mensajes y documentos en forma electrónica.
- Capa Financiera, o de medios de pago, asociada a los intercambios de información, bienes, servicios y seguridad.

El Comercio Electrónico a través de Internet está madurando y puede representar ventajas para el usuario. Una de ellas será la renovación de la infraestructura que da soporte a la Red; mayores anchos de banda, nuevo hardware en el lado de los servidores y la globalización (reducción del costo

de propiedad y mantenimiento) de tecnologías como RDSI. La venta eficaz en Internet pasará por la edición de catálogos electrónicos llenos de recursos multimedia y una excelente seguridad son la única posibilidad para atraer un buen número de compradores reacios a abandonar hábitos tradicionales.

5.2. TRANSACCIÓN COMERCIAL ELECTRÓNICA

Bajo el concepto que es una transacción comercial, muchas de las actividades soportadas por las infraestructuras de telecomunicación están relacionadas con la facturación y el pago. El objetivo último de todas estas actividades es conseguir en un futuro muy próximo un procedimiento seguro, rápido y global de pagos de bienes y servicios, lo que incluye el intercambio de información, es decir, asegurar las transacciones comerciales de forma electrónica.

Las transacciones se producen generalmente entre las empresas (B2B), entre éstas y sus clientes (B2C) o entre las empresas y las diferentes administraciones. Es ello que el Comercio Electrónico, es un concepto que abarca un amplio rango de actividades cuyo denominador común es que abarca todo el ciclo completo de la transacción comercial.

Entre los agentes que participan en una transacción comercial electrónica cabe destacar los roles de:

- Cliente: usuario que accede al sistema para adquirir un bien o servicio.

- Vendedor: persona física o jurídica con capacidad para comercializar un bien o servicio.
- Infraestructura telemática: redes y equipos de interconección entre los agentes.
- Medio de pago: tarjetas, cheque electrónico; dinero digital (E-cash); etc
- Centro autorizador: proveedor del servicio que intermedia y asegura la validez de la operación.
- Bancos y entidades financieras: papel intermediador autorizando los pagos online y ofreciendo garantías de seguridad en las transacciones.

5.3. VALIDEZ Y SEGURIDAD DE LAS TRANSACCIONES

La seguridad es una de las características que hasta ahora han retrasado las aplicaciones de Comercio Electrónico, por ello hasta ahora hay una necesidad de conseguir accesos y transacciones seguras y por tanto válidas para la realización de negocios. En todos los casos, la principal limitación hasta ahora ha sido la necesidad de asegurar la confidencialidad de las comunicaciones y autenticar que el cliente que interactua en la red es quien dice ser.

En la actualidad muchos comercios que existen ya en Internet han visto conveniente otorgar como forma de acceso e identificación un password a sus clientes.

5.4. CRIPTOGRAFIA.

Debemos entender por Criptografía (Kriptos=ocultar, Graphos=escritura) la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos **criptograma** o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina **algoritmo de encriptación**.

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, sobre todo en el campo militar y en aquellos otros en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros.

El primer sistema criptográfico como tal conocido se debe a Julio Cesar. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la letra situada tres posiciones por delante en el alfabeto latino.

Hay que destacar dos sistemas generales de ocultación, ya que juntos forman la base de muchos de los sistemas criptográficos actuales. Son la sustitución y la permutación.

La **sustitución** consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición natural en el alfabeto.

La **transposición** en cambio consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición en el orden del mensaje.

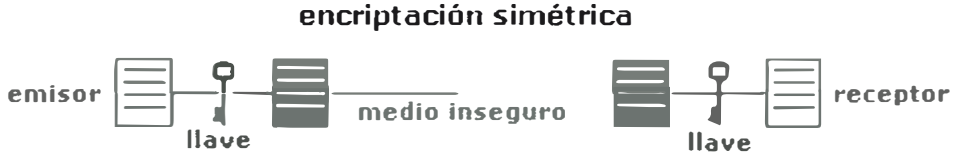
En la era moderna esta barrera clásica de la criptografía se rompió, debido principalmente a los siguientes factores:

- velocidad de cálculo: con la aparición de los computadores se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos.
- avance de las matemáticas : que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.
- necesidades de seguridad: surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la Criptología experimentó un fuerte avance.

A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, que se clasificaron en dos tipos, los de clave simétrica y los de clave pública. Los modernos algoritmos de encriptación simétricos mezclan la transposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

Criptografía simétrica.-

Incluye los sistemas clásicos, y se caracteriza por que en ellos se usa la misma clave para encriptar y para desencriptar, motivo por el que se denomina simétrica.



Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es importante y fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto.

Criptografía de clave pública.-

También llamada asimétrica, se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado.

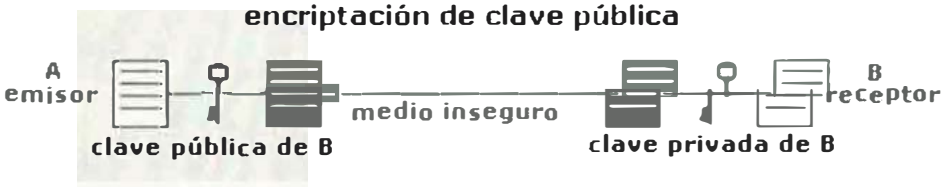
Generalmente una de las claves de la pareja, denominada **clave privada**, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada **clave pública**, utilizada para desencriptar el mensaje cifrado.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas

matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.



En este sistema, para enviar un documento con seguridad, el emisor (A) encripta el mismo con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por B. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

DES (Data Encryption Standard) esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado

normalizado para redes de ordenadores. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

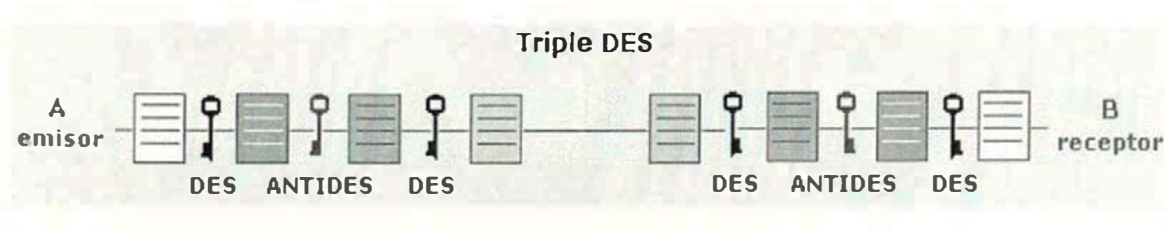
En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

El sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave.

Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (**TDES**), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si sé encripta el mismo

bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:



1. Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.

2. Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.

3. Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

Si la clave de 128 bits está formada por dos claves iguales de 64 bits (C1=C2), entonces el sistema se comporta como un DES simple.

VI. PROCESO DE TOMA DE DECISIONES

6.1. PLATEAMIENTO DEL PROBLEMA

6.1.1. INFORMACIÓN

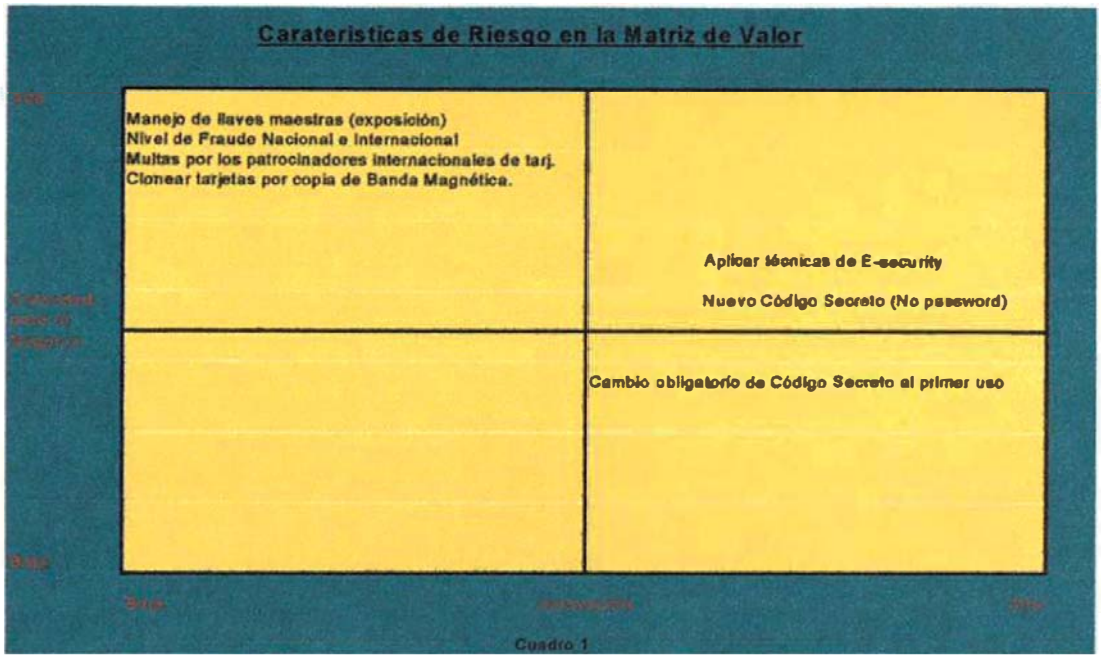
De acuerdo a los procesos detallados en el capitulo 4 se ha determinado una serie de deficiencias en el proceso físico de generación de tarjetas, así mismo en la utilización del código secreto generado para la tarjeta en la pagina web del banco, se detalla a continuación los principales problemas a superar.

- Software utilizado para la generación de los archivos con el cual se producen las tarjetas de crédito tiene incorporado las llaves maestras de seguridad como parte del código fuente, esto contraviniendo las normas internacionales de seguridad.
- El almacenamiento de las llaves maestras para la generación de las tarjetas de débito se encuentra en un repositorio lógico.
- Proceso de generación e impresión de códigos secretos (PINES) que no cumple con los estandares exigidos por las marcas patrocinadoras de las tarjetas como son VISA y AMERICAN EXPRESS.

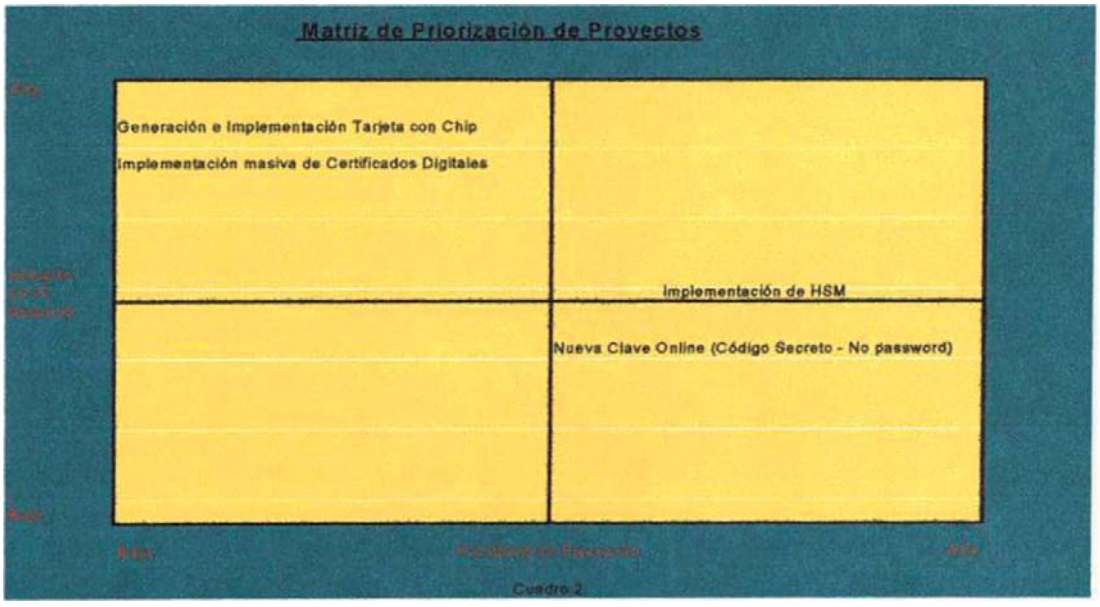
- La utilización del código secreto entregado por el banco al tarjetahabiente en todos los medios electrónicos, lo cual incluye Internet donde no se evidencia presencia física de la tarjeta.
- Método de generación de código secreto no aleatorio y con una antigüedad de más de una década.
- Los operadores del área de producción de tarjetas tienen la posibilidad de visualizar los códigos secretos al momento de la impresión del mismo.
- Limitadas transacciones financieras en el site del banco, solo se permite al tarjetahabiente efectuar transferencias entre sus propias cuentas, los pagos de servicios tienen limites de monto.
- Incremento del fraude a nivel internacional.

6.2. ALTERNATIVAS DE SOLUCIÓN

El análisis de la implantación de esta solución se basa en la Matriz de Valor (ver cuadro 1).



Además se presenta el análisis de priorización de proyectos con la Matriz respectiva (ver cuadro 2).



Para dar solución al problema planteado se ha visto conveniente definir dos estrategias básicas, estas son:

- Mejorar la seguridad en el proceso de generación de tarjetas.
- Permitir al cliente generar su propio código secreto a usar en el site del banco.

6.2.1. Estrategia 1.

Mejorar la seguridad en el proceso de generación de Tarjetas.

Alternativa 1.

Mejorar los niveles de seguridad existente con nuevos controles y desarrollos por software.

Desventaja:

Solución momentánea, no se cumple con superar las observaciones de auditoria interna y patrocinador de la marca de emisión de tarjetas (Visa, American Express).

Costo - Tiempo:

Desarrollo aproximado de $ 5.000,

Tiempo aproximado de implantación 2 meses.

Alternativa 2.

Implantación de un Módulo Central de Seguridad (HSM) para la generación de las tarjetas, seguridad por Hardware.

Ventaja:

Se cumple con las disposiciones de seguridad y de la marca de las tarjetas.

Costo – Tiempo:

Adquisición de Hardware, Software y desarrollo de interfases con un costo aproximado de $40.000,

Tiempo aproximado de implantación 4 meses.

Alternativa 3.

Migración a tarjetas inteligentes (Chip), por su esquema de alta seguridad.

Ventaja:

Tecnología de última generación que ocasionará cambios de hardware a nivel de toda la red (ventanillas, atm, pos, etc.)

Costo – Tiempo:

Cambios de hardware a nivel de la red e implantación de software, costo aproximado de $ 12.000.000,

Tiempo aproximado de implantación 18 meses.

6.2.2. Estrategia 2.

Permitir al cliente generar su propio código secreto a usar en el site del banco.

Alternativa 1.

Implementar un password para transacciones de pagos o transferencias a terceros.

Desventaja:

Un password no cubre los niveles de seguridad deseados, siempre es almacenado en medio electrónicos físicos.

Costo – Tiempo:

Adecuación de las aplicaciones actuales costo aproximado de desarrollos $ 9.000,

Tiempo aproximado de implantación 3 meses.

Alternativa 2.

Generación de una clave online de mayor longitud y con los niveles de seguridad similares al actual código secreto usado en otros canales.

Ventaja:

Generación de clave online con estandares existentes, no se almacena el código en ningún medio físico.

Costo – Tiempo:

Adecuación de las aplicaciones costo aproximado de desarrollos $ 9.000,

Tiempo aproximado de implantación 3 meses.

Alternativa 3.

Autenticación de transacciones mediante el uso de chip.

Desventaja:

Migración a tarjetas inteligentes con chip que contenga aplicación propietaria para la autenticación garantizando la presencia de la tarjeta en transacciones por Internet. Costo – Tiempo:

Desarrollo de aplicación propietaria en el site y en el chip de la tarjeta, costo aproximado $ 8.000,

Costo tarjeta c/chip de $ 4, a $ 6,

Dispositivo lector de chip para la PC del cliente costo $ 30,

Tiempo aproximado de implantación 6 meses.

6.3. METODOLÓGIA DE SOLUCIÓN

6.3.1. DEFINICIÓN DE PROCESOS DE LA SOLUCIÓN

El banco tiene como política fundamental el ofrecer a sus clientes productos y servicios de excelente calidad, por ello basado en la tecnología se busca las mejoras alternativas que permitan cumplir con su objetivo de calidad.

Precisamente el avance de la tecnología permite en la actualidad que la seguridad de claves sea administradas, guardadas y validadas bajo hardware, estos dispositivos electrónicos seguros están a prueba de intromisión ya que en caso que suceda esto su contenido es automáticamente destruido. Esto permite cumplir con los estandares internacionales de seguridad vigentes en la actualidad.

La tecnología también a permitido que el banco cree su propia pagina web donde sus clientes pueden efectuar consultas y transacciones de los diferentes productos que tenga.

Así mismo la tecnología de la información ofrece diversos esquemas de seguridad para autenticar las transacciones que realiza un cliente en el canal internet, algunos de estas alternativas son:

- Uso de password
- Certificado Digitales

La alternativa que se ofrece más adelante como solución es la generación de un código secreto en línea algo novedosa que esta basado en el mismo esquema que con el cual se obtiene los códigos secretos de las tarjetas bajo hardware.

6.3.1.1. MEJORAR LA SEGURIDAD EN EL PROCESO DE GENERACIÓN DE TARJETAS.

Descripción general.

El Host Security Module (HSM) (para una mejor comprensión en el Anexo 1 se tiene un Glosario de Términos Usados), es un aparato o periférico para computadora resistente a intrusión, si este dispositivo es abierto se borran las claves de encriptación maestra (LMK Local Master Key).

Las funciones de seguridad basadas en criptografia, son procesadas proveyendo funciones criptográficas para generar transacciones seguras en este caso, generar los pines o códigos secretos para tarjetas de débito y crédito, de tal modo que solamente el titular de la tarjeta podrá conocerlo al abrir el PINMAILER o sobre conteniendo su clave.

Algunas de las características básicas que debe reunir esta solución son las siguientes:

- Procesador criptográfico
- Certificación por los patrocinadores internacionales de tarjetas (VISA, American Express).
- Manejo de llaves de seguridad
- Generación de PVV (Personal Verification Value) calculado

Para que este dispositivo funcione correctamente y cumpla con las recomendaciones de Seguridad, se debe desarrollar el "Sistema de Generación" que es un software personalizado a las necesidades de manejo y control de información que requiere el banco.

Implementar esta solución nos permitirá realizar el proceso de impresión de PINES a través de un hardware especial que proporciona mayor seguridad a este proceso.

Adquisición del Host Security Module HSM (Caja RACAL)

El Host Security Module es un dispositivo o equipo de cifrado DES (Data Encription Standard un algoritmo de cifrado de dominio publico, publicado por el US National Bureu of Standard y adoptado por el American National Standard Institute ANSI) a prueba de manipulación indebida, provee seguridad a través de los medios seguros de cifrado necesarios para generar los valores criptograficos de tarjetas como PVV así como la generación confiable de los PIN's (Personal Identification Number) y PIN Mailers. El equipo debe ofrecer la conexión con el Host con interfaces seriales, Ethernet o IBM.

Adquisición y desarrollo del Sistema de generación PINADMIN

El Sistema de Generación o PIN ADMIN consiste en una aplicación de PC con un dispositivo PCSM (versión del Host Security Module para PC) que se utiliza internamente para la generación segura de claves. Esta solución que viene siendo desarrollada por la empresa **ELECTRODATA S.A.C.** debe contemplar las siguientes funciones:

- Flexibilidad en el manejo de las configuraciones para el formato de impresión y configuración del PIN Mailer.

- Funcionalidad en el proceso de impresión de manera que se impriman los dígitos configurando los espacios y transcripción verbal de ellos.
- Envío de PVV al HOST para el archivo Maestro del SAT (Sistema Administrador de Tarjetas), esté deberá ser calculado por cada número de tarjeta.
- Compatibilidad con American Express, permita configurar un card system especial para el procesamiento de pin mailers y generación de PVV's para tarjetas American Express.
- Generar una impresión dummy para verificar que la configuración de la impresión sea la adecuada, también debe permitir generar data de prueba para realizar las validaciones de las configuraciones realizadas sin necesitar recibir esta data de prueba desde Host.
- No debe existir limites para la cantidad de "Card System" que se pueden generar y configurar en el sistema.
- Control de Acceso al nivel de aplicación que maneje usuario y password para validar el ingreso al sistema.
- Manejo de Auditoria por Input File, el archivo debe registrar el Input File que se ha procesado.
- Manejo de Auditorias por Acciones, guardar información de los usuarios que acceden a la solución que, cuando, quien realiza algún evento.
- Manejo de eventualidades en el proceso, capacidad para seleccionar las tarjetas que se desean o no desean imprimir, selección individual de 1 a 10 cuentas.
- Capacidad para quebrar el archivo para programar el proceso de

impresión en etapas o lotes por operador. Esta función debe permitir realizar el proceso de impresión de los PIN MAILERS por excepción ya sea por rangos o identificación de tarjetas hasta 20 tarjetas individualmente.

- PINMAN debe contar con un "Validador" que se active si el proceso de envío de conformidad se duplica.

Esta solución supondrá adquirir el siguiente hardware y software:

- IBM PC o compatible (Host) Pentium o similar
- Sistema Operativo Windows NT versión 4.0

Se debe establecer el proceso de configuración del HSM y el ingreso de llaves de seguridad por parte de los custodios autorizados por la institución.

Adquisición Impresora Matricial para la impresión de los PIN MAILERS

Para realizar el proceso de impresión de PIN Mailers es necesario contar con hardware adecuado que realice el proceso de impresión a alta velocidad, para que esta nueva función no signifique un deterioro de los estándares de servicio de la Unidad de Producción de Tarjetas.

Las alternativas de solución evaluadas nos indican que un equipo optimo para realizar esta función es el que comercializa la empresa SYSTEM SUPPORT & SERVICES S.A. y que describimos a continuación:

- Impresora **IBM 6400 Line Matriz** Velocidad de 500 líneas por minuto cubierta con gabinete acústico.
- Puerto de comunicaciones serial
- Puerto paralelo Centronix Bidirideccional

- Memoria RAM de 04 MB
- Tecnología de impacto línea matricial con martillos cilíndricos tridimensionales.
- Frecuencia de trabajo de 24 horas continuas
- Modo de impresión en forma serial con presencia de cinta para amortiguar el martillo.

La adquisición de esta impresora serial que debe ir conectada al HSM implica realizar un cambio en la ubicación actual de los equipos de producción de tarjetas, ya que es definitivo que el espacio físico sé vera afectado. Del mismo modo será necesario capacitar a un recurso de Producción de Tarjetas en el manejo de puertos seriales, conocimientos de Administración de claves criptográficas, conocimiento de HSM en su instalación y operación.

El área responsable de programar la adquisición de esta impresora es el Servicio Procesamiento de Valorados.

Diseños de Card Carrier y PIN MAILER

Actualmente el proceso de impresión del PIN y códigos VISAPHONE de la tarjeta de crédito se realiza durante el proceso de embozado, personalización y encarte de la tarjeta utilizando el equipo **Datacard 9000** y el formulario card-carrier especialmente diseñado para cumplir la función de presentar la tarjeta de crédito y la información confidencial del cliente (PIN, Código VISAPHONE).

Implementar el proceso de generación e impresión de claves bajo HSM implica tener que diseñar un nuevo formato o PIN MAILER volviendo al antiguo sistema de uso de formulario F4864 08-93, conformado por un sobre totalmente cerrado y una hoja adicional.

La información básica que viaja realizará sobre la base de este diseño.

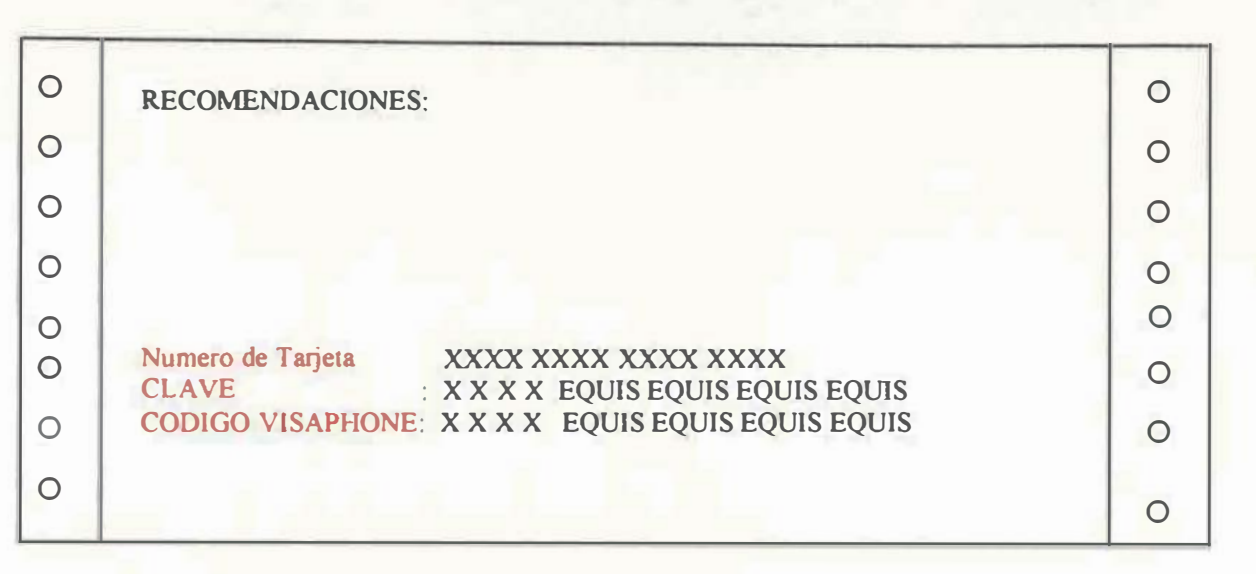
Se debe realizar el desarrollo para que la información referente al nombre del TH, PAN, Numero correlativo para la parte exterior del sobre, código VISAPHONE y dirección se encuentren disponibles de acuerdo al diseño de los sobres.

DATO	VISA	AMEX
Nombre	21 caracteres	21 Caracteres
Correlativo	16 caracteres	16 caracteres
PAN	16 caracteres	15 caracteres
VISA PHONE	4 caracteres	No Aplica
Dirección	30 caracteres	30 caracteres

1.- CONTRA HOJA utilizada para realizar el proceso de impresión, revestida en papel carbón o papel químico en el área donde van los nombres, tarjeta y dirección.

2.- Parte Externa del sobre que recibe el cliente.

3.- Parte interna donde se imprime el PIN y el Código VISAPHONE



Algoritmo de generación del PVV, VISAPHONE y CVV2 para instalar el proceso en HSM

La implementación de esta solución contempla adecuar la secuencia actual para generación del PVV usado para proporcionar chequeo criptografico sobre el contendido de la banda magnética de una tarjeta. Las PVV son creadas usando PVK clave DES algoritmo de cifración de dominio publico.

El HSM tiene la capacidad de generar el PVV que será transmitido al host para ser registrado en el archivo Relacionador de Tarjetas de la aplicación Sistema de Administración de Tarjetas (SAT) que también se encarga de la función de validar el PIN y el PVKI.

Concluida la etapa de generación de los PVV e impresión de los PINMAILERS se iniciara el proceso de embozado.

Se debe establecer claramente la secuencia de transmisión de datos desde el host hacia el servidor, al HSM, al equipo Datacard 9000 y luego la actualización en Host. Mayor detalle de este proceso será revisado mas adelante.

Las claves a emplear son de tres tipos ZMK, PVK's y CVK's. Todas son almacenadas o ingresadas al software encriptadas bajo la LMK previamente cargada en el HSM. Los PIN's generados son encriptados bajo la LMK, y las claves PVK's y CVK's son además encriptadas bajo la ZMK.

Las claves no son desencriptadas en ningún momento por software es decir, cualquier función de encriptación será procesada a través del HSM y es este quien envía a la impresora los PIN mailers a través de su puerto serial. Lo que nos da un nivel muy alto de seguridad empleando hardware para el procesamiento de encriptación.

Se mantendrá el modo actual de generación del Código Visaphone, siendo este parte del INPUT FILE, debiendo ajustarse su posición dentro del PINMAILER.

Método de generación de PINES bajo modalidad 'Random'

La generación de PINE's puede ser realizada bajo dos métodos: el modo IBM que consiste en generar el mismo PIN cuando los parámetros de generación como PAN es el mismo y es el que empleamos actualmente.

Nuestra solución empleara el método RANDOM, este método nos garantiza que el PIN o Clave secreta que llegue al cliente siempre será único, cada vez que el sistema tenga necesidad de generar un PIN este será totalmente

diferente. Este método que es nuevo tiene sus implicancias ya que si nuestros clientes están acostumbrados a recibir la misma clave cuando realizan una regrabación de tarjetas a partir del momento de implementar esta solución esa funcionalidad dejara de ser efectiva.

Las tarjetas Visa a diferencia de las tarjetas American Express no diferencian al titular de la cuenta de los adicionales, actualmente las tarjetas crédito Visa no emiten PIN para las tarjetas adicionales. Cuando se implemente la generación de PINES bajo HSM no debe generar PINES para las tarjetas de crédito Visa adicionales de manera similar al esquema actual.

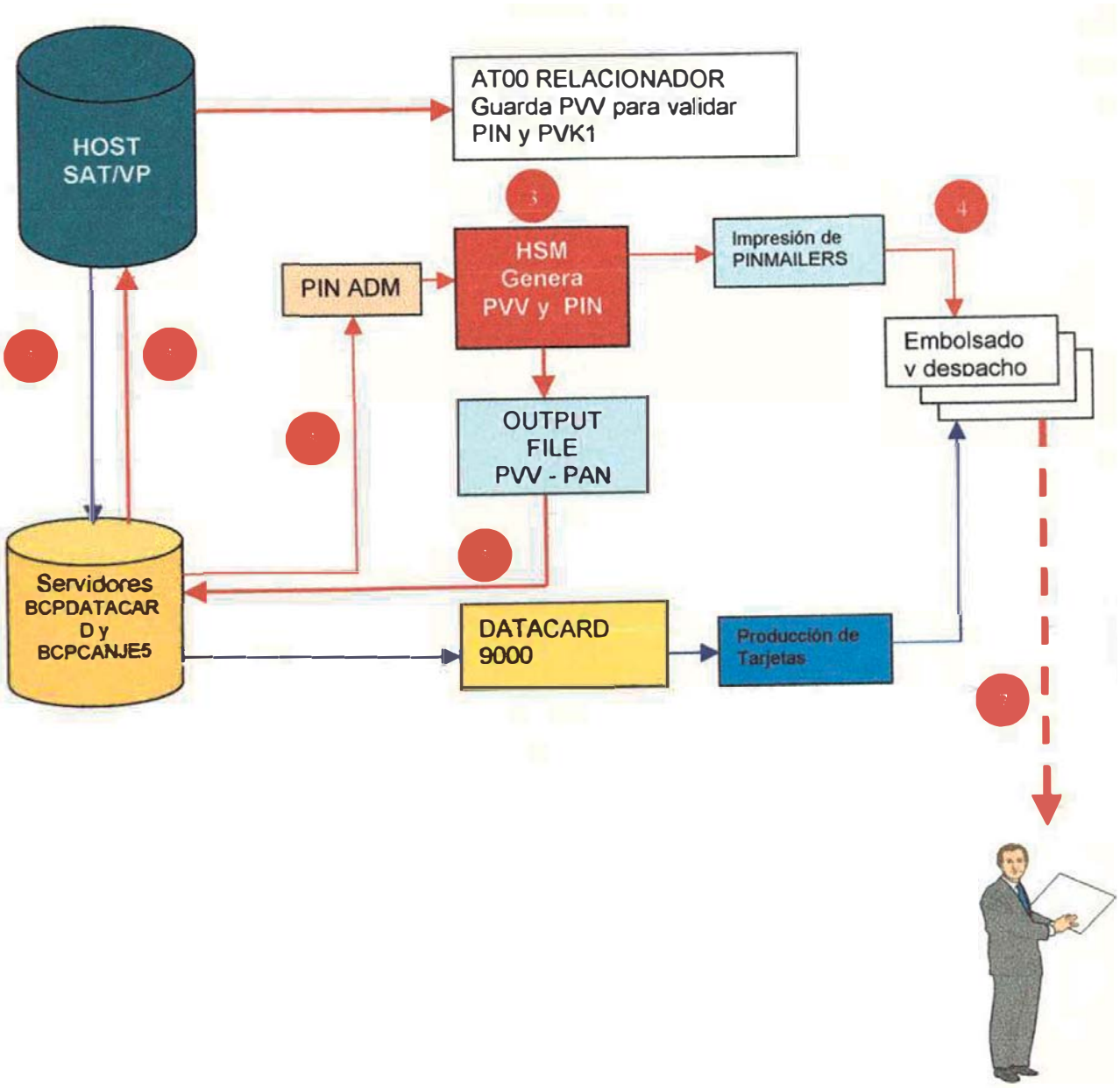
Para el caso de las tarjetas adicionales de la marca American Express el criterio es distinto ya que el archivo Maestro del SAT si guarda el numero de tarjeta o PAN de la tarjeta adicional que es diferente al del titular. Por consiguiente el HSM generará los PVV de estas tarjetas antes de la carga del archivo a la DC9000 y posterior envío a Host.

Evaluación de espacio físico y recursos adicionales para atender el proceso de impresión y ensobrado de PINES.

La implementación de esta solución trae consigo una serie de cambios así como asumir nuevas funciones en la Unidad de Producción de Tarjetas, dentro de estos cambios está el diseñar una nueva distribución del espacio físico así como la ubicación e instalación de los nuevos equipos consistentes en PC; HSM e impresora matricial, espacio para guardar los sobres PINMAILERS y espacio seguro para guardar los PINMAILERS ya impresos. Esta actividad se hará en coordinación con el área de Seguridad de

Información quienes recomendaran la manera mas apropiada de disponer los nuevos equipos y los ya existentes así como disponer la implementación de los equipos de monitores y seguridad. (cámaras, sensores y otros).

Diagramas de procesos.



En el acápite numero 4.2.4.3 se explicó el actual proceso de emisión y reposición de tarjetas de crédito y débito, el diagrama de la pagina anterior esquematiza dicho proceso e incluye los nuevos pasos a implementar, los cuales se detallan a continuación:

PASO 1

- Las aplicaciones de tarjeta de crédito y débito generan la información de las nuevas tarjetas a producir.
- Se transfiere el archivo que contiene la información de las tarjetas al Servidor de la Data Card 9000.

PASO 2

- Servidor recibe la información remitida por el computador central.
- Se ejecuta un proceso de desdoblamiento de la información remitida, un archivo es almacenado en el servidor a ser usada en el paso 5 y el otro se transfiere a la PC que tiene el software PIN ADMIN.

PASO 3

- El operador de tumo define que tipo de tarjetas va a procesar.
- Se prepara físicamente la impresora con el formato (PINMAILER) que corresponda a la tarjeta a procesar.
- La aplicación PINADMIN procesa la información tarjeta por tarjeta, entregando la información al módulo físico de seguridad (HSM).
- El módulo de seguridad (HSM) genera el código secreto (PIN) y valores a grabase en la banda magnética de la tarjeta, estos son almacenados en un archivo a ser usado en el paso 5.

PASO 4

- Los sobres con los códigos secretos son remitidos a la sección despacho.
- La sección Despacho para el caso de las tarjetas de crédito procede a la distribución respectiva a los clientes.
- Para el caso de las tarjetas de débito la sección Despacho, junta con los sobres que contienen la tarjeta generada en la Data Card 9000.

PASO 5

- La aplicación PINADMIN transfiere el archivo que contiene los valores de seguridad indicado en el paso 3 al servidor de la Data Card.
- La información recibida del PINADMIN se junta con la información remitida por el computador central, esto mediante un proceso automatizado.
- También la aplicación PINADMIN genera otro archivo que contiene los valores (PVV) a ser transmitidos al computador central.

PASO 6

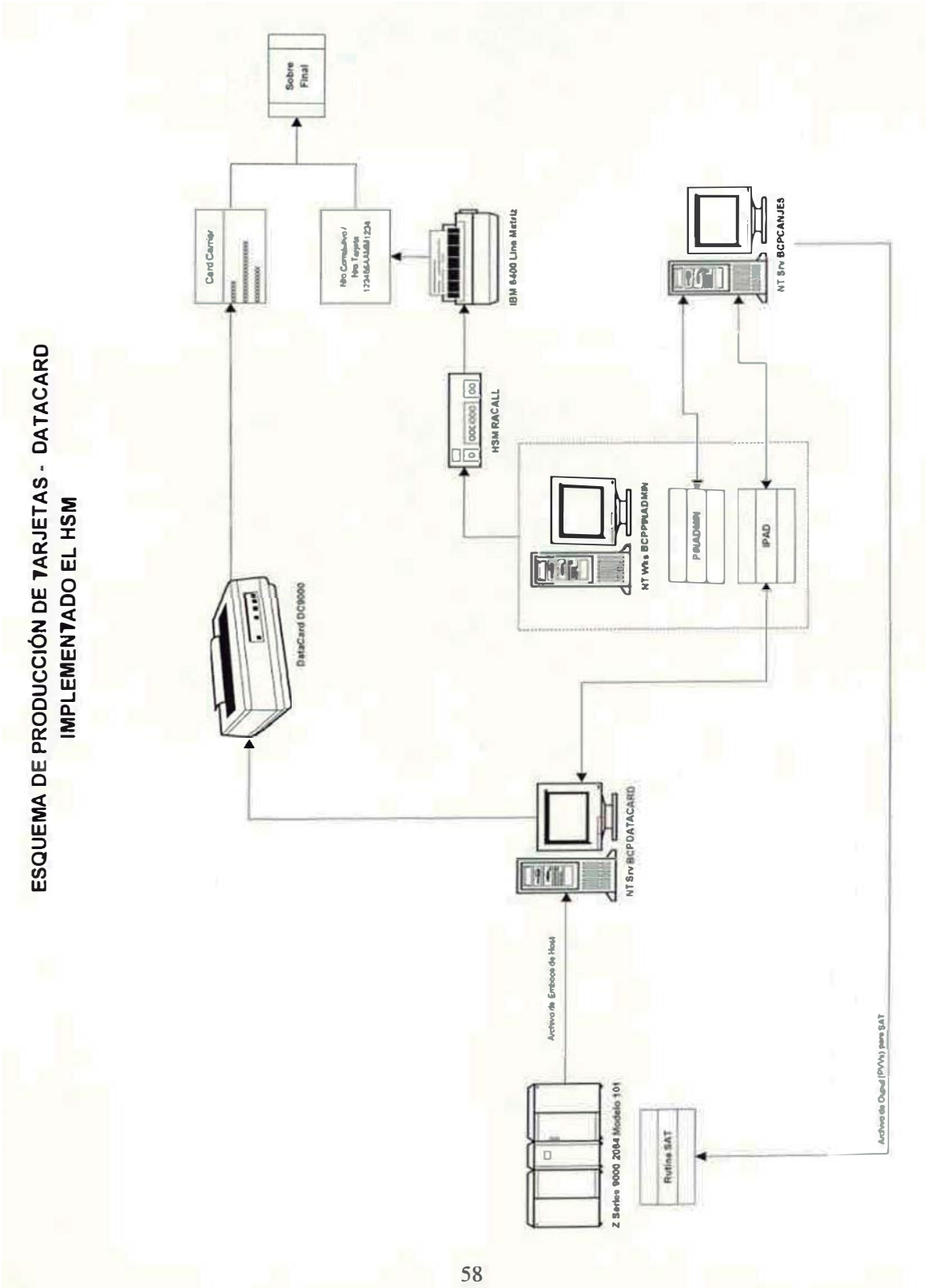
- Se transmite la información al computador central.
- La aplicación SAT (Sistema de Administración de Tarjetas) recibe la información y mediante un proceso batch se actualiza el archivo Relacionador con los valores PVV que se empleará en la validación de cada tarjeta y poseedor de la misma.

PASO 7

- Vía correo las tarjetas de créditos son entregadas al cliente en forma separada la tarjeta y el PINMAILER.

- Las tarjetas de débito y su código secreto son entregadas en las oficinas del banco.

En el gráfico adjunto se muestra la arquitectura de la solución.



Proceso y Funcionalidad del PIN ADMIN

Descripción Funcional que debe cumplir el sistema de Generación de PINE's

- Políticas de conexión para el acceso a los archivos de llaves (pinadmin.set), logs, inputs y outputs. Las rutas de dichos archivos serán definidas en la política del Servicio de Seguridad de la Información del banco (Valor Texto)
- Presentar un input file por cada CardSystem y rutina de desdoblamiento del archivo que baja de host.
- Presentar dos usuarios de red (UsrPinManAdmin y UsrPinMan) para accesar a los archivos indicados en el punto anterior. Ambos usuarios sólo pueden ser ingresados desde la máquina donde se encuentra instalada la aplicación (política **logon to** de NT)

Aplicación	Llaves	Logs	Outputs	Inputs
UU UsrPinManAdmin	Change	Change	Change	Read
UsrPinMan	Read	Change	Change	Read

- Mostrar alguna ventana u opción que permita al operador visualizar el check value de la llave.
- La PC donde se instale el PinAdmin, será configurada de acuerdo a las políticas de seguridad necesarias para que el usuario solo pueda accesar al aplicativo PinAdmin.
- El orden de los iconos se presentará en orden secuencial de acuerdo al

proceso de impresión de pines. Primero el icono del Embosser y luego el de PrintMailer.

- Tendrá desarrollado la funcionalidad de impresión de pruebas
- No tendrá la función de manejo de usuarios dentro del PinAdmin. Toda la administración será a través del Servicio de Seguridad de la Información.
- Presentará el perfil Padm_Configurador (perfil de desarrollo).

6.3.1.2. PERMITIR AL CLIENTE GENERAR SU PROPIO CÓDIGO SECRETO A USAR EN EL SITE DEL BANCO

Descripción general.

Se elaborará un Módulo de Generación y Cambio de Código Secreto en línea, esto permitirá a los clientes que usan el Internet y en forma particular el portal del Banco contar con un nuevo código secreto de mayor longitud y diferente al entregado por el banco.

El código entregado por la institución sólo será utilizado al momento de generar su nuevo código secreto en línea y por única vez.

Funciones por procesos.

SAP ->	INTERNET ->	RECAUDACIONES->	MAIL
Firma Contrato	Deja Solicitud	Activa Clave Online	Envía mail
Marca 'Contrato'	Marca 'Clave'	Marca 'Afiliado'	

En cada canal, por la que pasa la solicitud se generan nuevos estados. Los estados son producto de las diversas combinaciones que generan tres marcas:

Marca 'Contrato':

- Esta marca se activa cuando el cliente ha firmado su contrato de afiliación al servicio de clave online.
- El único canal por el cual se activa esta marca es a través de Plataforma.

- La Asesora activa manualmente el campo en SAP, pero la marca va a SAT en línea.

Marca 'Clave':

- Esta marca se activa cuando el cliente genera su clave online en Internet, la cual se guarda en SAT en línea.
- El único canal por el cual se activa esta marca es a través del site 'Tus Cuentas' - Internet (módulo G2C).
- La activación es automática (por el sistema).

Marca 'Afiliado':

- Esta marca se activa cuando Recaudaciones ha recepcionado la solicitud de Plataforma y procede a habilitar el servicio de la clave online.
- El único canal por el cual se activa esta marca es a través de Recaudaciones.
- El digitador de recaudaciones activa manualmente el campo en SAT, pero la marca va a SAT en línea.

Los estados existentes son:

Estado	Marca		
	Contrato	Clave	Afiliado
NONE			
INACTIVO	X		
POR ACTIVAR	X	X	
ACTIVO	X	X	X
CANJE	X		X

None: Aquel cliente que no ha realizado ninguna acción para solicitar su clave online.

Inactivo: Aquel que ya firmó su contrato en plataforma pero aún no ha generado su clave online.

Por activar: Aquel cliente con status 'Inactivo' que ya genero su segunda clave por Internet.

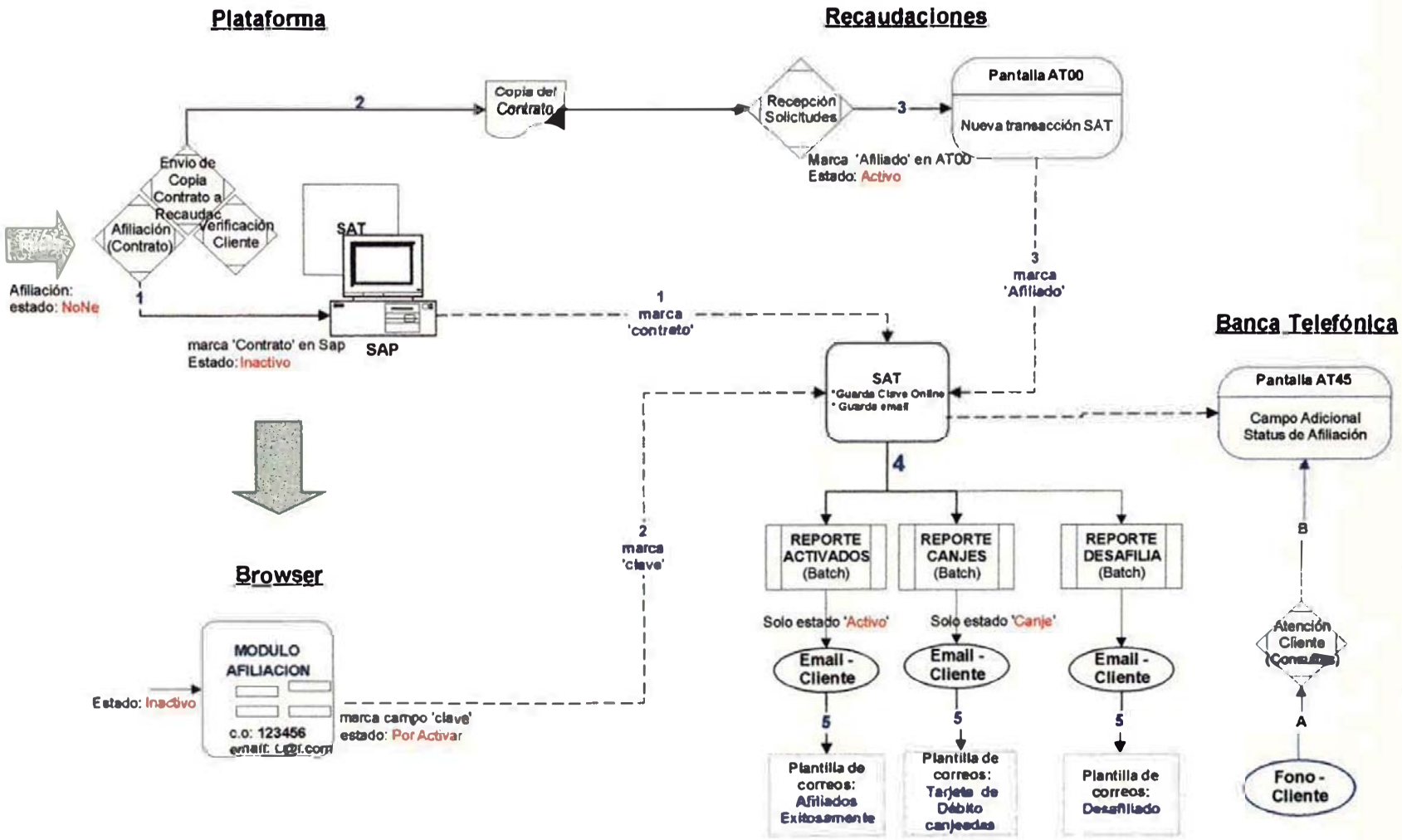
Activo: Aquel cliente con status 'Por activar' que ya fue activado por Recaudaciones.

Canje: Aquel cliente 'Activo' que por diversos motivos a canjeado su tarjeta de Débito por una nueva.

Esa nueva tarjeta heredó las marcas 'Contrato' y 'Afiliado' de la anterior, pero no hereda la marca 'clave'. Por ende pasa a un estado 'canje', hasta que el cliente digite a través de internet su nueva clave online y vuelva a su estado ACTIVO inicial.

Cabe destacar que, no existen estados diferentes a los mencionados en el cuadro superior, por ende SAT, SAP y HBK deben de controlar que no se generen estados distintos a los mencionados.

DIAGRAMA DEL PROCEDIMIENTO DE SERVICIO : CLAVE ONLINE



Este diagrama detalla el procedimiento a seguir en la afiliación al servicio de clave online.

PASO 1

- El cliente se dirige a Plataforma de Atención para que verifiquen su identidad, efectúen la firma del contrato de afiliación y envíen la copia del mismo hacia Recaudaciones.
- La plataformista deberá marcar en SAP que se recepcionó la solicitud (marca 'contrato') para cada tarjeta en forma independiente.
- Estado Input: 'NONE' - Estado Output: 'INACTIVO'.

PASO 2

- La idea es que el cliente genere su clave online a través de Internet.
- Se genera automáticamente la marca 'clave'.
- Estado Input 'INACTIVO' - Estado Output 'POR ACTIVAR'.
- Del mismo modo, mientras el cliente va generando su clave online, la copia del contrato de afiliación está viajando a Recaudaciones.

PASO 3

- Recaudaciones recepciona las solicitudes y procede a activar manualmente tarjeta por tarjeta ingresando la marca 'afiliado'.
- La activación se hace en una nueva pantalla del AT00.
- Estado Input 'POR ACTIVAR' - Estado Output 'ACTIVO'.

PASO 4

- Al final del día a través de un Reporte Batch se identificará a los nuevos clientes Afiliados (status ACTIVO) y se les enviará un mail de conformidad de activación al nuevo servicio "clave online".

- Se deberá generar un reporte batch de los clientes activos que canjearon la tarjeta afiliada (status CANJE) para el envío de su correspondiente mail.
- Finalmente a través de reporte batch se identificará a aquellos clientes que han sido Desafiliados en el día (Cambio de estado ACTIVO a NONE).

BANCA TELEFONICA

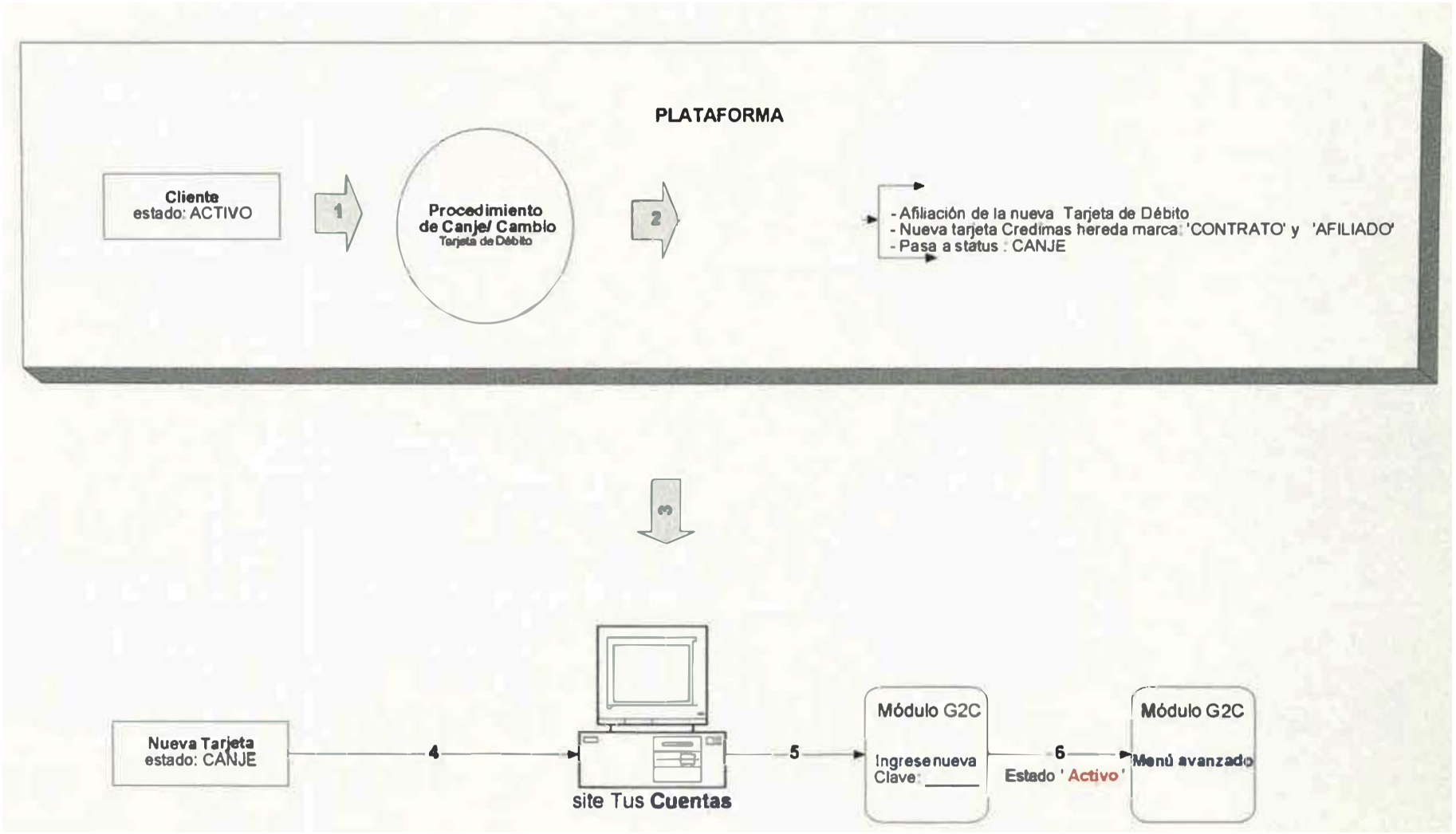
Existe la opción Consulta de Tarjetas por Número es mediante esta opción del SAT que Banca Telefónica responda consultas de los clientes referente a su estado actual de afiliación a clave Online.

A: El cliente llama consultando.

B: Recepcionista de Banca Telefónica mediante la Consulta de Tarjeta por Número informa al cliente el estado de la Clave Online.

DIAGRAMA DE CANJE DE TARJETAS de DËBITO

Para canje de tarjetas anteriormente activas al servicio de Clave Online



Este diagrama denota los casos en los que clientes con estado 'ACTIVO' proceden a canjear su tarjeta, ya sea por extravío, pérdida, deterioro del físico, etc.

El procedimiento de canje ya existente, indica que el cliente deberá ir a Plataforma y canjear su tarjeta anterior por una nueva.

Dicha nueva tarjeta, por rutina del SAT hereda las propiedades de la anterior (todas las marcas, excepto la marca 'clave'), pero no hereda el valor PVV2 de la clave online.

Por ese motivo, dicha nueva tarjeta poseerá el estado CANJE con las siguientes marcas:

- Contrato
- Afiliado

Aquellas tarjetas con este estado (canje) deberán ingresar a Internet a generar su nueva clave online, con la cual activarían la marca 'clave' faltante y volvería a su estado ACTIVO inicial.

CASOS DE OLVIDO DE CLAVE

Para aquellos casos en los que los clientes olvidan su clave online deberán acercarse a plataforma de atención para que canjeen su tarjeta por otra.

DESAFILIACION AL SERVICIO

Para aquellos casos en los que el cliente desee desafiliarse del servicio de clave online, deberá ir a plataforma de atención al cliente a firmar un contrato de desafiliación, la copia de dicho contrato viajará a recaudaciones y finalmente el personal de dicha área procederá a desafiliarlo manualmente, regresándolo al estado NONE.

Eliminación de datos "clave Online"

"Consiste en borrar los datos de la clave online guardados en la ampliación del archivo SAT (Cabe resaltar que no se modifica nada del PIN), y a su vez, quitarle la marca a la tarjeta, de modo que, pase al status NONE".

Este esquema no debe impedir que a posteriori el cliente pueda re-afiliarse al servicio, siguiendo el mismo procedimiento.

Este esquema se aplicará en los siguientes casos:

Clave Expirada

Cuando el cliente haya solicitado en plataforma el servicio y aún no haya generado su clave online en intemet. Por ende nunca paso del estado INACTIVO a POR ACTIVAR.

Internamente, el sistema diariamente deberá detectar aquellas tarjetas que se encuentran en status 'INACTIVO' por un periodo mayor a 15 días calendario, para proceder a ejecutar el esquema de eliminación.

Función Desafiliación

Es una función que solo tendrá el personal de recaudaciones y que sirve para desafiliar a aquellos clientes que ya no deseen el servicio. Internamente SAT limpia todas las marcas que posea dicha tarjeta (en el estado que estuviera) dejando la tarjeta en NONE.

Si a posteriori, el cliente se quisiera volver a afiliar, los nuevos datos de la tarjeta (como clave online ó email) serán generados nuevamente en el SAT.

Bitácoras de auditoría (LOGS).

- Log de bloqueo de clave online - HBK.
- Log de modificación status - SAT.

- Ampliar el LOG de transacciones administrativas del SAT
- Log de las solicitudes efectuadas a través de Internet.

Procedimiento de Afiliación al Servicio de clave online

Descripción de la ampliación del archivo SAT y creación de cimientos para la clave online

El archivo Maestro del SAT deberá soportar:

- Campos de validación del PIN. (Ya existentes e inmodificables).
- Nuevos campos de validación de la clave online. (A desarrollar en este proyecto).

Se ampliará el archivo Maestro del SAT para la generación de los campos de validación de la clave online, se emularán aquellos ya existentes del PIN.

El cliente digitará en el "módulo G2C" la "clave online" deseada. Dicha clave será de **6** cifras numéricas, e ingresará a la rutina BCSS, de modo que, genere el valor a guardar en el campo PVV2 de la "Clave Online" del SAT. Para ello se construirá nuevos cimientos similares a los del PIN DE 4, pero para una clave de 6.

El nivel de seguridad de este proceso, es el mismo de la generación del PIN de la tarjeta de débito.

Nótese que, los campos de validación del PIN actual "NO DEBERAN SER AFECTADOS, NI MODIFICADOS", en ningún sentido durante la implementación de este proyecto.

Cabe resaltar que para los casos de canje de tarjetas "Activas" se procederá a pasarlos al estado "Canje" para que luego ingresen su clave online deseada.

Descripción del Proceso de firma del Contrato – Sistema Adm.de Productos.

Personal de plataforma de ventas seguirá un procedimiento especificado. Este procedimiento básicamente consiste en que Plataforma de Atención al cliente deberá:

- Recepcionar al cliente interesado en afiliarse al servicio.
- Del mismo modo, deberá informar a los nuevos clientes del Banco sobre la existencia del servicio.
- Verificar la autenticidad del cliente, solicitándole original y copia de DNI y tarjeta de débito.
- Efectuar la firma del contrato de afiliación al servicio "clave online". Este Contrato es un block que tiene pre - impresas los diferentes tipos de tarjetas que se pueden afiliar al servicio clave online.
- Marcar en SAP a dicha tarjeta en el campo 'Contrato', cambiando al estado 'INACTIVO'.
- Envío de constancia al área de Recaudaciones para que activen la marca 'afiliado' luego de que el cliente genere su clave online en internet.

Nótese que el sistema solo posibilitará efectuar la marca 'Contrato' siempre y cuando la tarjeta se encuentre en el estado 'NONE'. Para los otros estados no será posible efectuar dicha marca. Esto se realizará en una pantalla SAT dentro de SAP. Cabe resaltar que se reutilizará la pantalla de CONSULTA SAP solo para casos en los que Plataformista desee consultar el status de clave Online de una tarjeta. SAT en todos los casos envía el status - no la marca.

Descripción del proceso de generación de clave onine en el site "Tus Cuentas" (G2C)

Dentro del site "Tus Cuentas" existirá un link al módulo G2C, el cual cuenta con una funcionalidad que le permite al cliente generar su clave online, siempre y cuando éste se encuentre en estado INACTIVO y tiene como finalidad el ingreso de algunos datos relevantes que se guardarán en Host para ser validados posteriormente.

Los campos más importantes del módulo G2C son:

- Campo "clave online": numérico, es un campo de ingreso, para que el cliente digite su segunda clave personalizada. La cual será guardada en SAT. Se implementará una clave de seis dígitos numéricos. Será una clave por tarjeta afiliada.
- E-mail: Para enviarle al cliente un aviso de que se encuentra afiliado al servicio (ACTIVO), que debe generar clave online (CANJE), y que ya esta DESAFILIADO del servicio. Es un email por tarjeta afiliada.

Al momento de solicitar el servicio por Internet, el sistema internamente deberá:

- Guardar todos los datos ingresados en SAT, para que puedan ser consultados en la opción Consulta de Tarjetas por Número del SAT por el área de Recaudaciones y Banca Telefónica.
- Guardar el "Personal Verification Value" (PVV2) de la "clave online", detallado en el "Proceso de ampliación del archivo SAT".
- Mantener en status "Por Activar" a dicha clave online, hasta que éste sea modificado manualmente en Recaudaciones, por el estado AFILIADO.

Finalmente el cliente deberá esperar hasta que se termine de activar dicha clave.

Si no ha ingresado en el módulo de G2C luego de 15 días que firmó el contrato, se deberá aplicar el EED (Esquema de eliminación de Datos).

Nótese que, esta funcionalidad sólo será mostrada a aquellos clientes con estado 'INACTIVO'. SAT entregará a HBK el dato de status.

Descripción del Proceso de Activación de claves online Recaudaciones

El área de Recaudaciones diariamente recibirá las copias del contrato, enviadas por Plataforma de Atención al cliente, y procederán a aprobarlos en el sistema.

Para ello, consultarán una nueva transacción dentro del menú principal del SAT, en donde efectuarán dichas aprobaciones.

Todas las copias del contrato que ingresen al área deberán ser habilitados indefectiblemente siempre y cuando en sistema SAT lo encuentren en el estado 'Por activar' o en caso contrario desactivar si así lo solicitó el cliente.

Para activar dicha clave Online, el personal de Recaudaciones deberá activar la marca 'Afiliado' de tal modo que, su estado de salida será: **ACTIVO.**

Todo el circuito de activación durará 24 horas útiles en Lima y 72 horas en provincias (Lo que tarde en llevar la copia del contrato a Recaudaciones y activar la clave online), y se deberá informar de ello al cliente en el procedimiento.

Se puede dar el caso, que una solicitud se extravíe en el recorrido de Plataforma y Recaudaciones, generando malestar en el cliente, que deberá volver a ejecutar todo el circuito de afiliación.

En el caso de las desafiliaciones, también tendrán una opción para retornar al status NONE a las tarjetas en cualquiera de sus status de input.

Dicha pantalla extraerá por número de tarjeta el status en el que se encuentra la tarjeta. Y a su vez permite modificar dicho status.

Descripción del Proceso de consulta de status - Banca Telefónica.

El cliente tendrá la posibilidad de saber en que status esta su solicitud de afiliación al servicio “Clave Online”. Con una llamada al personal de Banca Telefónica, se le puede informar en que situación se encuentra.

Para ello, se deberá ingresar a la opción de Consulta de Tarjeta por número del Sistema Administración de Tarjetas, consultar los campos:

- Campo ‘status’,
- Campo "Fecha y Hora" para cada status.

Cabe señalar que, Banca Telefónica no tendrá capacidad de modificar el status en el que se encuentre un cliente, sólo visualizarlo.

Descripción del Proceso de generación de Reporte Batch y archivo Host.

Se deben generar diariamente tres reportes Batch:

REPORTE BATCH ACTIVADOS

Se debe generar un listado de tarjetas que han sido activadas durante cada

día calendario. De tal modo que, esta información nos sirva para enviarle un mail automático de conformidad a los clientes.

Para ello, la rutina de SAT, al final del día deberá generar un reporte llamado "Reporte de Clave Online", con el listado de todas las tarjetas que hayan adquirido el status 'ACTIVO en el transcurso de ese día.

Este reporte a su vez debe generar un archivo HOST para que sea transmitido al servidor winnt con SQL mail .(Envío de correos).

REPORTE BATCH CANJEADOS

Se debe generar un listado de tarjetas que se encuentren en el status CANJE durante cada día calendario. De tal modo que, esta información nos sirva para enviarle un mail automático al cliente indicando que debe generar su clave online.

Para ello, la rutina de SAT, al final del día deberá generar un reporte llamado "Reporte de Casos de Canje para Clave Online", con el listado de todas las tarjetas que hayan adquirido el status 'CANJE' en el transcurso de ese día.

Este reporte a su vez debe generar un archivo HOST para que sea transmitido al servidor winnt con SQL mail. (Envío de correos).

REPORTE DE DESAFILIADOS

A aquellos clientes que en el día pasaron del estado ACTIVO a NONE, por ejecución de dicha función a cargo de recaudaciones, se les deberá enviar un correo electrónico informándoles que ya no están afiliados al servicio de clave online.

Se debe seguir el mismo procedimiento de envío, es decir, un reporte Batch que se enlaza a una plantilla de correo para su posterior envío.

Descripción del Proceso de e-mails de confirmación.

Finalmente el archivo HOST de tarjetas afiliadas en el día, por Recaudaciones deberá ser llevado al servidor de correos, para que éste automáticamente proceda a lanzar los mails, enviándole al cliente confirmación de que ya se encuentra activado para utilizar su clave online. Del mismo modo para el reporte Host de Canjeadas y para las desafiliadas.

Cada tarjeta afiliada o canjeada, que este en los correspondientes archivos Host estarán asociadas a una plantilla de correos la cual tiene datos genéricos y específicos de cada cliente.

El envío de e-mails será diariamente a las 06:00 a.m. de cada día calendario.

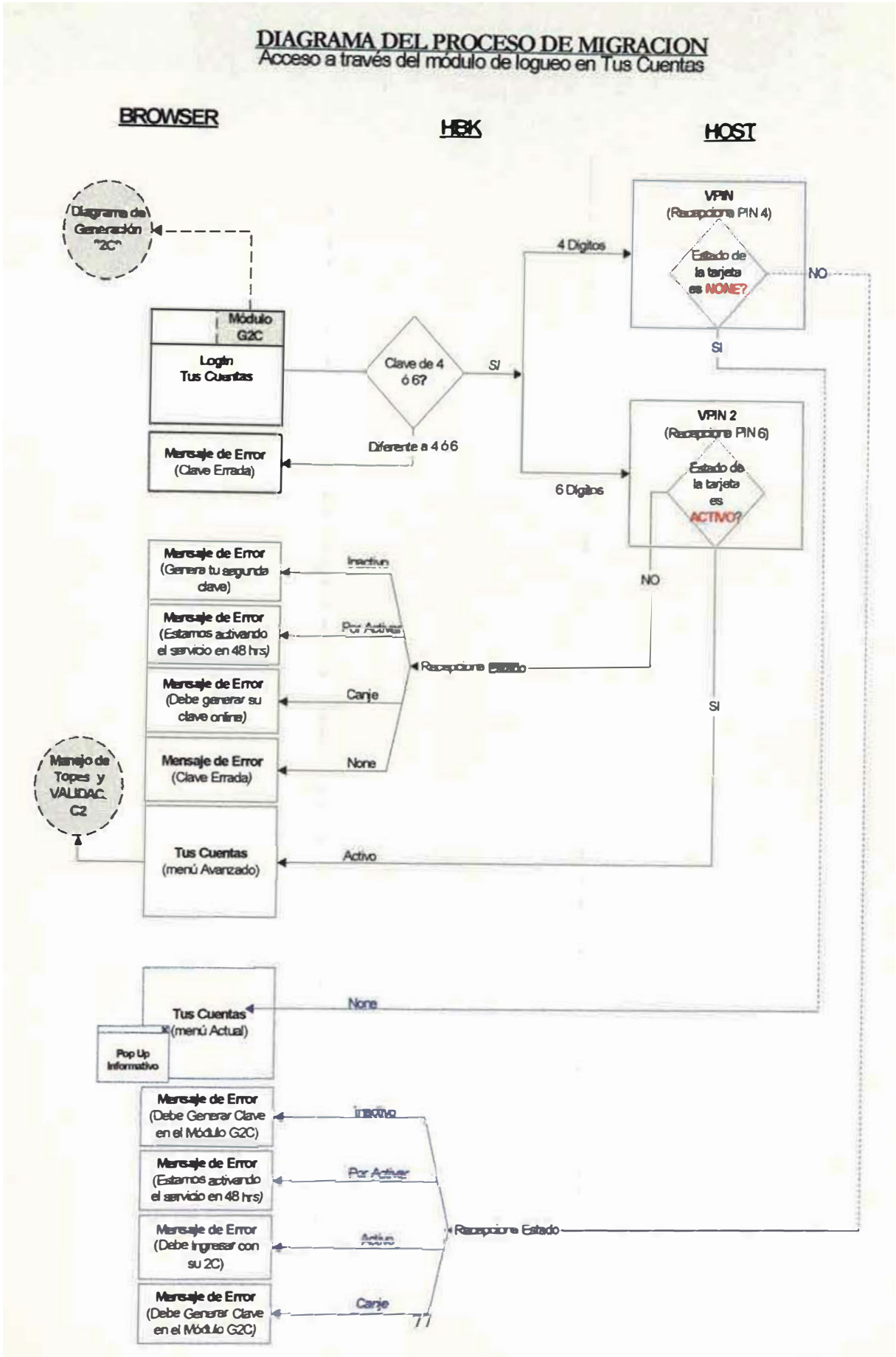
Descripción del Proceso de desafiliación del servicio.

Si el cliente ya no desea estar afiliado al servicio, bastará con que asista a plataforma de atención, y firme el contrato de desafiliación, el cual viajará a Recaudaciones para una "Desafiliación" manual.

Descripción del proceso olvido de clave.

Si este es el caso, el cliente deberá ir a plataforma a canjear su tarjeta, con lo cual pasaría a estar en el estado CANJE.

DIAGRAMA DEL PROCESO DE MIGRACION
Acceso a través del módulo de logueo en Tus Cuentas



Proceso de Migración en "Tus Cuentas"

Este proceso de migración durará desde la puesta en producción de este proyecto hasta la fecha de corte fin de dicha migración. Comercialmente se han definido 60 días. Al final de este proceso, entrará en vigencia la nueva lógica de acceso a "Tus Cuentas".

Descripción del proceso

En la pantalla principal de Tus Cuentas coexistirán dos módulos:

1) La pantalla de Login
2) El módulo G2C.

Ambos tendrán diferente lógica, en este caso detallaremos el primer módulo.

En la pantalla login, el cliente podrá ingresar su PIN o su clave online. HBK deberá identificar la longitud de la clave (4 ó 6 ó diferente a ambas). De ser diferentes, se emitirá un mensaje de error correspondiente.

En caso que sea una clave de 4, la enviará a la transacción de validación del pin actual "VPIN", y si es de 6 HBK derivará a la trama de validación de la clave online "VPIN2".

Transacción VPIN:

Valida el pin actual

La trama cuando llegue a Host deberá verificar si el estado de la tarjeta es NONE o no. En caso de serlo, HOST le entregará ese dato a HBK y éste mostrará el menú actual de Tus Cuentas conjuntamente con algunas pantallas Pop Up de publicidad.

En caso de no ser none, igualmente HOST le entrega el estado de dicha

tarjeta a HBK para que éste muestre la pantalla de error conveniente por estado. En este caso al cliente no se le permite el acceso a Tus Cuentas.

En el gráfico es toda la parte azul del diagrama.

Transacción VPIN2:

Valida la clave online - NUEVA TRANSACCION.

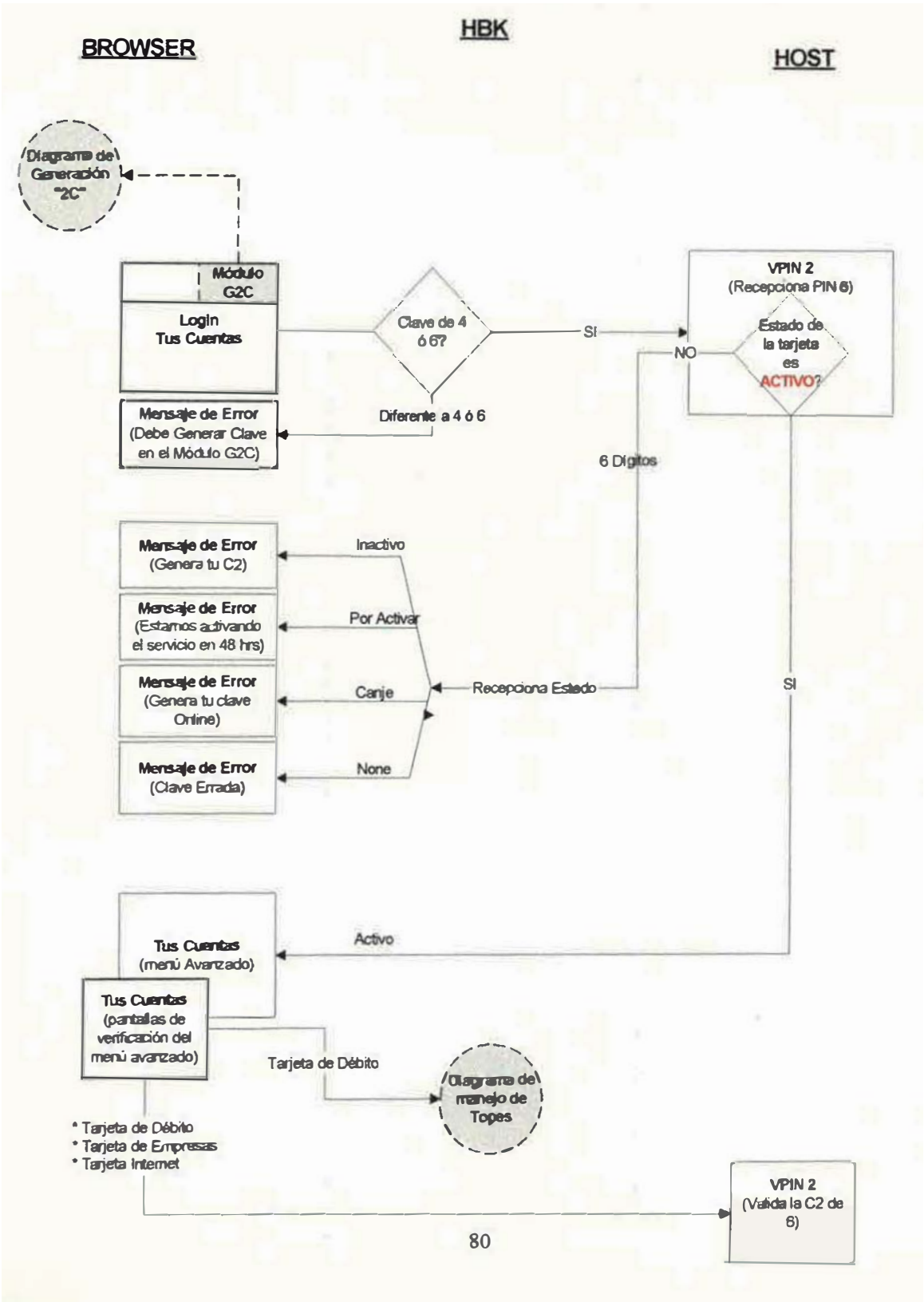
La trama cuando llegue a Host deberá verificar si el estado de la tarjeta es ACTIVO o no. En caso de serlo, HOST le entregará ese dato a HBK y éste mostrará el menú avanzado de Tus Cuentas, el cual poseerá la lógica de verificar todas las operaciones del menú de Débito con esta clave online.

En caso de no ser activo, igualmente HOST le entrega el estado de dicha tarjeta a HBK para que éste muestre la pantalla de error para cada caso. En este caso no se le permite el acceso Tus Cuentas del cliente.

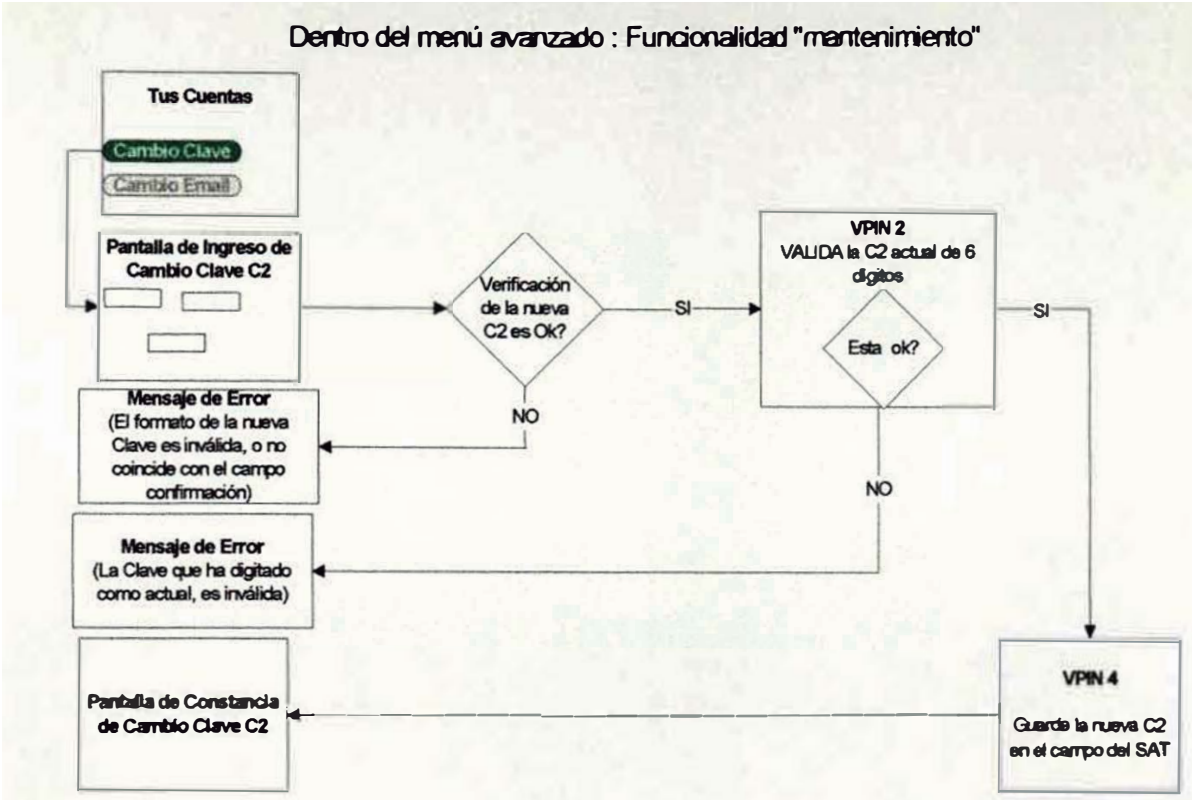
En el gráfico es toda la parte de color negro del diagrama.

DIAGRAMA LOGIN FUTURO DE TUS CUENTAS

Finalizado el proceso de Migración



CAMBIO DE CLAVE C2



CAMBIO DE EMAIL

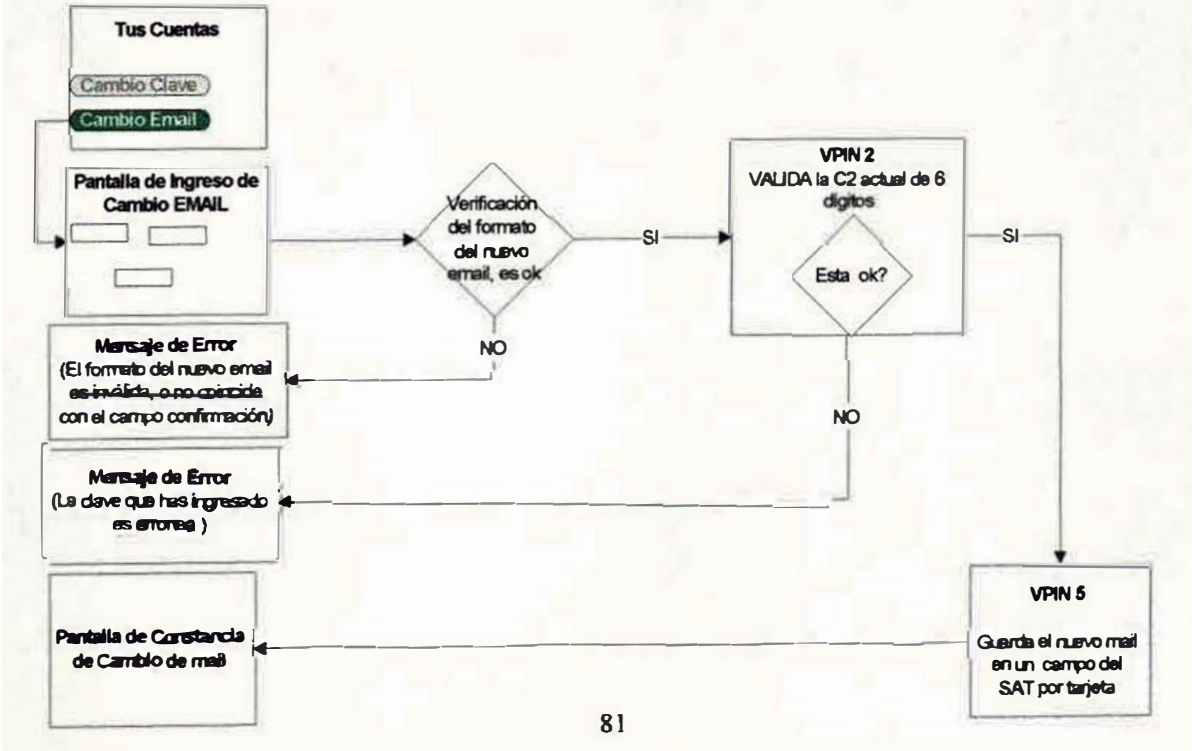
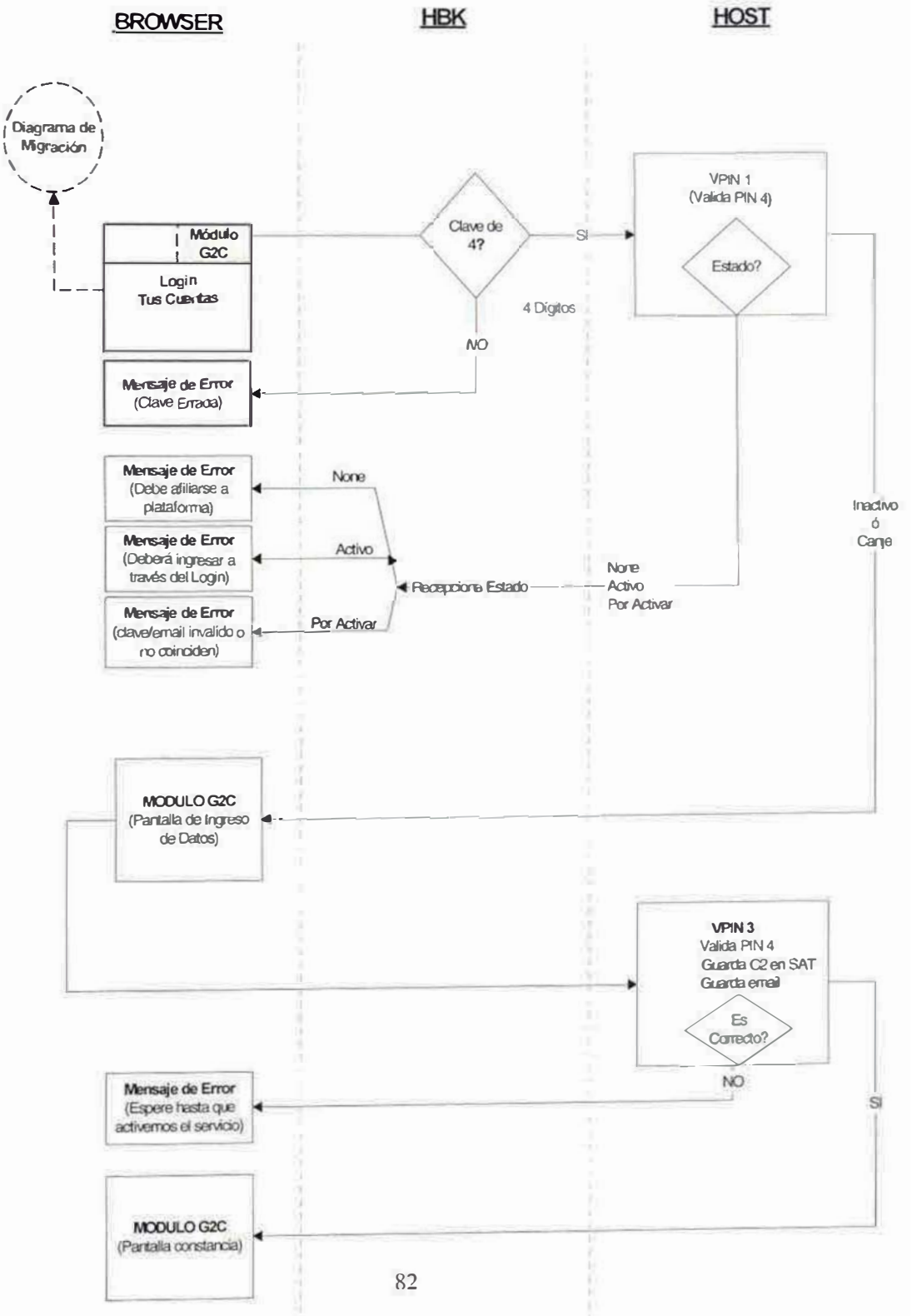


DIAGRAMA DEL GENERACION DE SEGUNDA CLAVE "G2C"

Acceso a través del módulo de Generación de clave en Tus Cuentas



Módulo de generación clave online en el módulo G2C

Descripción del proceso

En el módulo de generación de la clave online, el cliente deberá digitar solamente su PIN, cualquier otra opción será rechazada por el browser. HBK deberá validar si es una clave de 4 dígitos o no.

SI ES CLAVE DE 4 DIGITOS

Deberá enviar a Host la consulta para que éste identifique el estado de dicha tarjeta.

Si el estado es inactivo o canje*:*

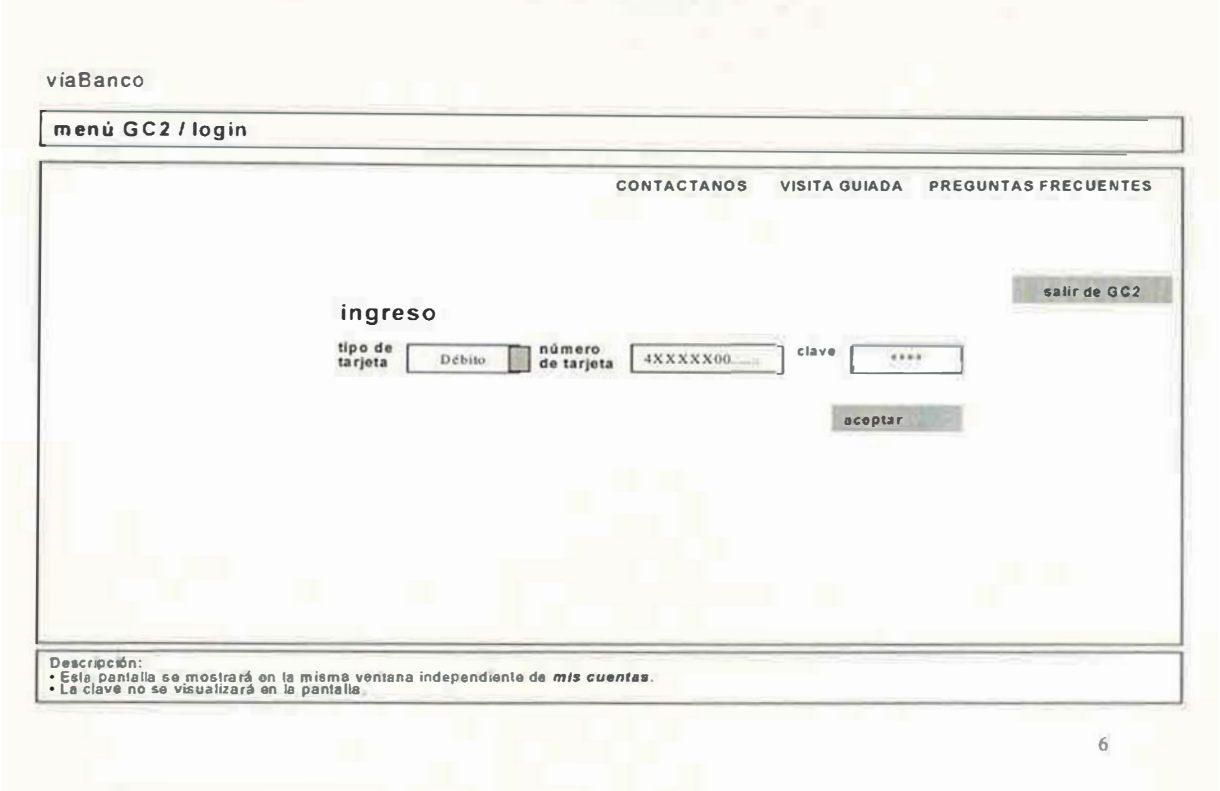
Se deriva la consulta a la transacción VPIN1 para la validación de dicha clave de 4 dígitos. De ser positiva la validación, se le muestra el menú del G2C para generar su clave online. En caso de ser negativa la validación, se envía un mensaje de error.

Si la validación es positiva y el cliente esta tratando de generar la segunda clave, los datos que ingrese en la "Pantalla inicial del G2C" deberá ser enviados a HOST para que ejecute la transacción VPIN3 "*transacción de G2C*". La transacción VPIN3: Valida el PIN de 4 dígitos, guarda la clave online en SAT y guarda el email del cliente también en SAT.

Si el estado es diferente a (inactivo o canje):

HOST enviará ese dato a HBK para que HBK muestre el mensaje de error mas adecuado en cada caso.

Módulo de Generación de Clave Online (G2C)



Pantalla de logueo al G2C

A esta pantalla sólo accederán los clientes Inactivos o Canje que deseen generar su segunda clave. El ingreso es a través del PIN de 4 dígitos.

Campos y Controles

Tipo de tarjeta: Para que el cliente seleccione en el combo que tipo de tarjeta para la cual generará la clave online. Las tarjetas que estarían en este combo box son:

- Débito Visa
- Débito Visa con chip
- Tarjeta Empresarial
- Tarjeta Internet

Campo número de tarjeta: Numérico de hasta 16 caracteres. Es para que el cliente ingrese el BIN de la tarjeta. Por defecto se mostrará los 8 primeros dígitos de las tarjetas de débito o Empresarial luego de la selección del combo (como actualmente se está mostrando en la pantalla de login actual de Tus Cuentas). Para la Tarjeta Internet se mostrarán solo los 6 primeros dígitos.

Campo clave: Es un campo de ingreso del PIN, su tamaño es de 4 caracteres numéricos. Se mostrarán asteriscos " * " por cada carácter ingresado.

Botón Aceptar: Valida que el cliente haya ingresado un PIN, y que esté correcto.

Salir de GC2: Sale de dicha pantalla y lleva al cliente nuevamente a la pantalla de login inicial.

Mensajes de Error

ME - 001: PIN errado

ME - 002: Debe acceder a Tus Cuentas si tiene clave online

ME - 003: Debe solicitar su clave online en Plataforma.

ME - 004: Debe ingresar a través de su pantalla de Login de "Tus Cuentas".

ME - 005: Espere hasta que le generemos el servicio.

Pantalla de ingreso de datos para generar la C2

Campos y Controles

Campo de ingreso de nueva clave online: Este campo, es de ingreso de la clave online que desee el cliente. Es numérico con capacidad de 6 dígitos los cuales deberán viajar encriptados a Host. No se mostrarán planos en esta pantalla. Obligatorio.

Campo confirmación de clave online: Idem del campo "clave online". Obligatorio.

Campo email: Para que el cliente ingrese la dirección electrónica en la cual desea recibir la conformidad de la afiliación. Es alfanumérico, de 40 dígitos entre los cuales aceptará sólo un carácter especial @ Obligatorio.

Campo Confirmación email: Idem del campo email. Obligatorio.

Campo “Ingreso de PIN”: Para que el cliente digite su PIN confirmando la operación.

Botón Aceptar: Validará que el campo “clave online” y el campo confirmación clave online sean iguales. Validará que el campo email contenga un simbolo @ obligatoriamente así como también que sea igual al campo confirmación de email. Validará el campo “Ingreso de PIN”

Salir de GC2: Cierra el módulo GC2. [Pantalla de despedida]

Mensajes de error

ME - 001: PIN Errado.

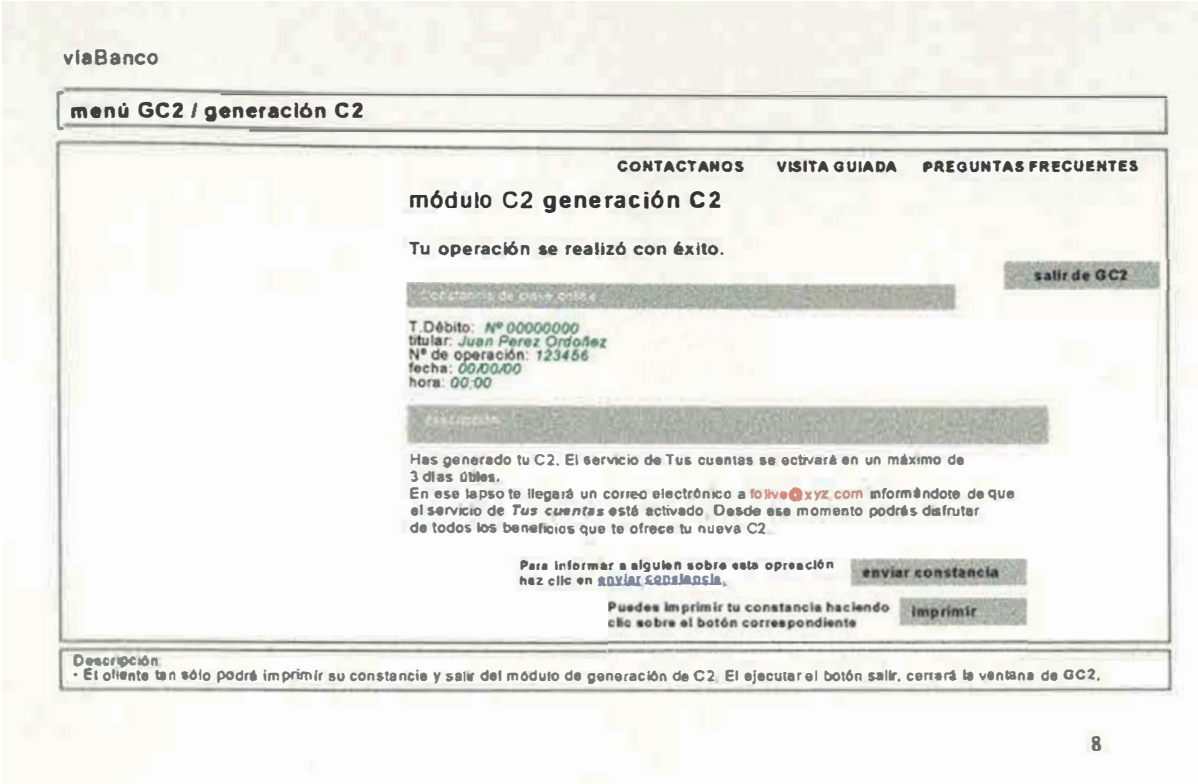
ME - 006: Formato de la nueva clave online no cumple con standar.

ME - 007: No coincide con el campo de confirmación de clave online.

ME - 008: Formato de email no coincide con estándar.

ME - 009: No coincide con el campo de confirmación de email.

Constancia de generación de la clave online.



Campos y controles

Se deberá mostrar los campos informativos de: número de T.Débito, Titular, Número de Operación, fecha y Hora. Del mismo modo un breve texto descriptivo para el cliente.

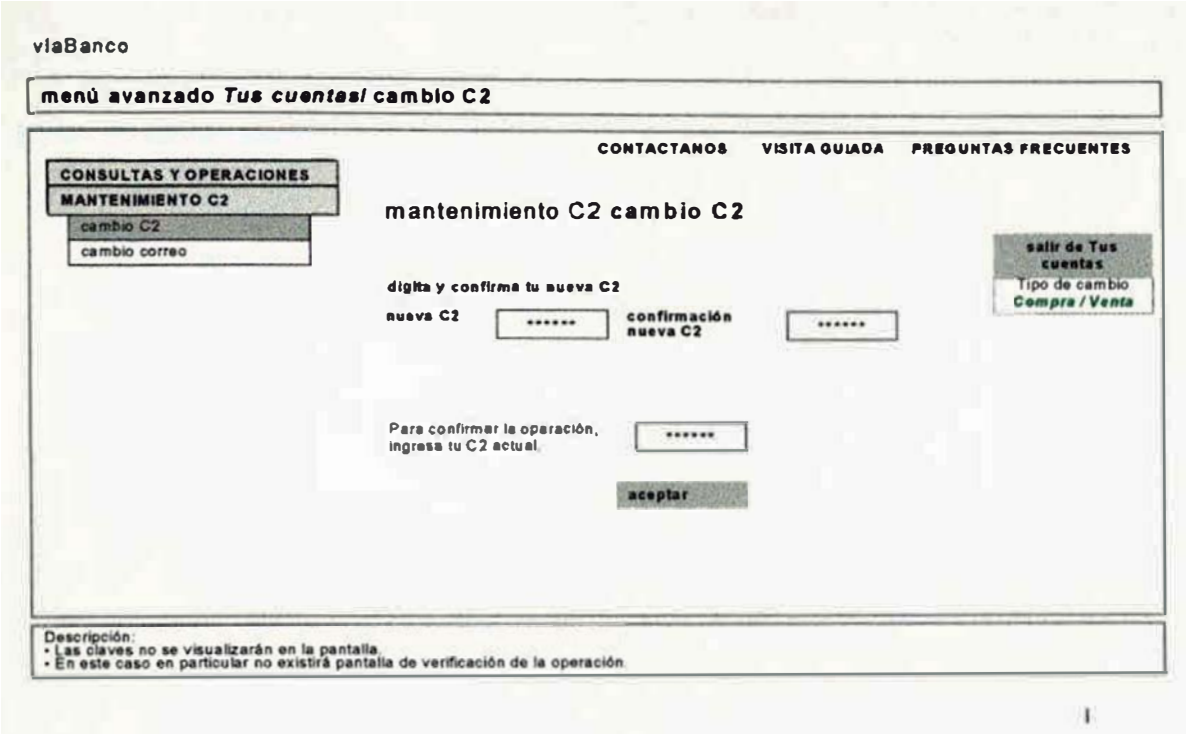
Botón Imprimir: Cumple la función de Impresión de constancia.

Envio de constancia a terceros: Cumple con la funcionalidad existente en Tus Cuentas.

Salir GC2.

Menú Avanzado - Funcionalidad "Mantenimiento"

Pantalla de Ingreso de datos para cambio de C2



Será una funcionalidad que en el menú avanzado estará debajo de "Mantenimiento". Sus cambios son en línea.

Campos y Controles

Campo de ingreso de nueva clave online: Este campo, es de ingreso de la nueva clave online que desee el cliente. Es numérico con capacidad de 6 dígitos los cuales deberán viajar encriptados a Host. No se mostrarán planos en esta pantalla. Obligatorio.

Campo Confirmación de clave online: Idem del campo 1. Obligatorio.

Campo de ingreso de actual clave online: El cliente deberá ingresar su clave online vigente que confirme dicha operación de cambio de clave online.

Botón Aceptar: Deberá verificar que el campo 1 tenga el formato estándar, que coincida con el formato 2 y validar que la clave online vigente sea la correcta.

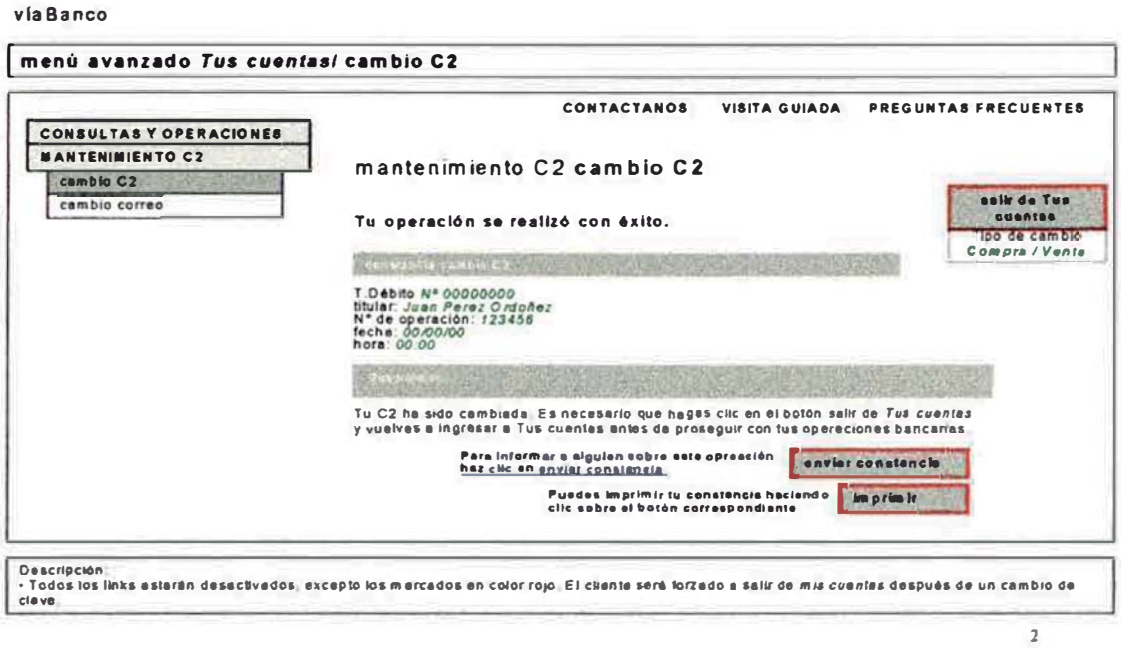
Mensajes de Error

ME - 006: Formato de la nueva clave online no cumple con standar.

ME - 007: No coincide con el campo de confirmación de clave online.

ME - 010: Clave online errada.

Constancia del cambio de C2



Campos y Controles

Se deberá mostrar los campos informativos de: Número de Tarjeta de Débito, Titular, Número de Operación, fecha y Hora. Del mismo modo un breve texto descriptivo para el cliente.

Botón Imprimir: Cumple la función de Impresión de constancia.

Envío de constancia a terceros: Cumple con la funcionalidad existente en Tus Cuentas.

Salir de Tus Cuentas.

Se deberá mantener solo activo los botones "Salir de Tus Cuentas", "Enviar constancia" e "Imprimir", las demás funcionalidades del menú no estarán activas de tal modo que se forzará al cliente a salir y reingresar a Tus Cuentas.

6.4. TOMA DE DECISIONES

La decisión de la institución bancaria fue dada por incursionar en la implantación de nuevo esquema de seguridad en el proceso de la generación de tarjetas con la implantación de módulo central de seguridad por hardware y también el permitir que sus clientes que usan su portal tenga la facilidad de ingresar en línea su propio código secreto.

Haciendo un Análisis de Beneficios y Costos respecto a la determinación adoptada se puedo decir:

Beneficios para la Institución Bancaria:

Cumplir con la recomendación del área de auditoria interna y de Visa Internacional.

Afianzar la calidad de servicios que se otorga a los tarjetahabientes del banco.

Fortalecimiento del portal de negocios por intemet al permitir a sus clientes generar su propio de código secreto.

Afianzar los servicios electrónicos personales desarrollados por el banco a fin de mantener el liderazgo de presencia por internet a través de los diversos medios de pagos que se ofrece a las personas naturales.

Beneficios para el cliente:

Acceder al portal del banco vía internet con un nuevo código secreto que el mismo cliente define y que no es almacenado en ningún medio físico o lógico.

Acceder a nuevas transacciones financieras como son las transferencias a cuentas de terceros.

Acceder a pagos de servicios con limites superiores a los actuales.

Costos para la Institución bancaria:

Costos establecidos en la adquisición del módulo central de seguridad (HSM).

Costos establecidos en la adquisición del software necesario para la solución.

Costos establecidos en la adquisición de la impresora que emite los PIN MAILER.

Costos establecidos en la adquisición de los PINMAILER.

Costos establecidos en la impresión de contratos para la nueva Clave Online.

Costos establecidos por el marketing y difusión por medios de comunicación masiva hacia los clientes anunciando los nuevos beneficios.

Costos para el cliente:

Obtención de un nuevo código secreto con cero costo de afiliación.

6.5. ESTRATEGIAS ADOPTADAS

6.5.1. Configuración de la cadena de valor

Establecimiento de las necesidades del cliente

- Acceder en línea a obtener su propio código secreto en una forma sencilla y segura en el portal que tiene el banco.
- Acceso a cambiar en línea su nuevo código secreto (Clave Online) cuando lo desee.
- Independizar o unificar su nueva Clave Online de todas las tarjetas

que posee con el banco.

- Acceso a nuevas transacciones financieras en el site del banco.
- Acceso a pagos de servicios con limites superiores a los actuales.

Establecimiento de actividades en la cadena de valor de la institución

Actividades Primarias:

Logística Interna:

- Adquisición de los equipos y software definidos en la solución.
- Adquisición del sobre de seguridad (PINMAILER) y envío al centro de producción de tarjetas.
- Envío de las tarjetas a sus respectivos centros de consumo (agencias a nivel nacional).

Producción:

- Realizar el proceso físico de grabación del plástico (tarjeta).
- Realizar la impresión de los PINMAILER.

Logística externa:

- Entrega y Distribución de tarjetas de débito a clientes utilizando la red de agencias a nivel nacional.
- Entrega y Distribución de las tarjetas de crédito a la dirección que indique el cliente.
- Entrega y Distribución de los PINMAILER de tarjetas de crédito a la dirección que indique el cliente, en forma independiente del plástico y utilizando otro proveedor del servicio de distribución como medida de seguridad.

Mercadotecnia y Ventas:

- Lanzamiento de la publicidad respectiva en medios de difusión masiva.
- Alinear el lanzamiento con la presencia de los cambios previstos en el portal del banco.
- Fortalecer la fuerza de ventas en funcionarios de atención a clientes en las agencias.

Servicio posventa:

- Atención de Consultas por medio de la Banca Telefónica
- Atención de Consultas y reclamos por medio de correo electrónico desde el portal.
- Identificar mejoras en la calidad de atención al cliente.

Actividades de Apoyo:

Financiamiento:

- Parte de los recursos se obtienen de las partidas definidas para la inversión y promoción del comercio electrónico.
- También se obtiene recursos de las partidas definidas para la continuidad operativa de tarjetas de débito y crédito.

Desarrollo Tecnológico:

- Adecuación del canal Banca Telefónica para la atención de las consultas del publico.
- Adecuación de las Plataformas de Atención al cliente para la atención presencial del publico.

Administración de Recursos Humanos

- Difusión y aplicación de la normativa para lanzar la solución del presente proyecto a todas las unidades de negocio comprometidas.
- Adiestramiento al personal de las plataformas de atención al cliente para ofrecer e instruir a los tarjetahabientes del uso de la nueva Clave Online.
- Adiestramiento al personal del área de producción de tarjetas para el manejo de los nuevos equipos y software instalados de acuerdo a lo indicado en el presente proyecto.

Infraestructura de la Institución:

Asuntos Legales

- Establecimiento del contrato de afiliación a la nueva Clave Online para su utilización en el portal del Banco.

Contabilidad

- Mantener el registro contable que existe.

VII. Evaluación de resultados

7.1. Situación Antes de la implantación del HSM y nueva Clave Online :

El banco muestra un escenario con cierto grado de incertidumbre en el proceso de producción de tarjetas y en el manejo de las llaves de seguridad, esto debido a una supuesta exposición de las mismas, ya que desde su instalación no han sido cambiadas como lo establecen los estandares internacionales.

La institución ha recibido recomendaciones de parte de su área interna de Auditoria, así también de los auditores de Visa Internacional, a fin de mejorar los controles en la manipulación de las llaves de seguridad con las que se generan las tarjetas de crédito y débito, se sugiere la implantación de nuevos esquemas se seguridad utilizando dispositivos electrónicos que existe para este fin, así también la instalación de nuevas llaves maestras en coordinación con Visa Internacional.

A inicio de este nuevo mileneo el banco ha incursionado a los Negocios Electrónicos con la implementación su portal de negocios sobre la Internet, esto ha permitido la generación de nuevos esquemas de pago.

La competencia esta preparando algunas iniciativas para incrementar o incursionar en el comercio electrónico sin un anuncio oficial al respecto para

la puesta en servicio a sus clientes y publico en general.

Los clientes tienen recelo e inseguridad de usar Internet, la principal razón esta definida por el tema de seguridad y el uso del código secreto que el banco otorga a los tarjetahabientes ya que es el mismo código secreto usado en otros medios electrónicos donde se exige la presencia física de una tarjeta.

7.2. Situación después de la implantación de la tarjeta :

Hace un año aproximadamente la institución bancaria confirmó su condición de líder en el mercado, lanzando la primera tarjeta para comprar en internet. Con ello se logra captar un gran número de nuevos clientes y a su vez se dio un gran impulso al comercio electrónico en el país.

La nueva Clave Online buscó satisfacer la necesidad de los tarjetahabientes que desean efectuar transacciones financieras por la internet de una forma segura. De esta forma junto con la estrategia de la presencia del portal de negocios, se logra aperturar la posibilidad de ofrecer nuevas transacciones financieras y productos, también ha permitido fidelizar a los actuales clientes.

Gratuidad de las operaciones financieras por internet a través del portal del banco esto debido a que no se cobran comisiones ni mantenimiento. Sin embargo, las mismas operaciones en otros canales tienen un costo establecido.

Desde el día del lanzamiento de esta solución ha recibido excelentes comentarios por las posibilidades de implementar nuevos productos y transacciones financieras.

Se ha detectado algunos impactos después de la implantación de esta solución que a continuación detallamos.

Mayor seguridad en el proceso de la generación de tarjetas superando las observaciones de auditoria interna y externa.

Mayor flexibilidad en brindar soluciones tecnológicas para la infraestructura del Banco.

Las transacciones con tarjetas por internet y en los diferentes canales electrónicos de la red del Banco afectan el nivel del servicio a través de un incremento sobre el promedio de atención diaria de transacciones financieras bajo el esquema de atención de 24 horas x 7 días.

Estimula al uso de la internet para realizar compras en diferentes categorías de empresas.

A través del portal del Banco se hace propicia nuevas relaciones con otras empresas al permitir pagos de servicios.

En el Anexo 2 se observa claramente la aceptación y evolución de las transacciones financieras en el portal del banco lo cual justifica plenamente la inversión realizada.

VIII. Conclusiones y Recomendaciones

Las tarjetas bancarias de uso electrónico sean de crédito o débito son el medio de pago alternativo para compras de bienes y servicios por el canal internet, el banco también ha incursionado en este medio electrónico creando su propio portal en donde ofrece sus productos y servicios.

Para llevar a cabo este propósito la institución bancaria dispone de la tecnología de información que la aplica a través de los diferentes puntos de contacto que tiene con sus clientes formales e informales.

La organización ha permitido fortalecer la unidad de negocios de comercio electrónico para impulsar a través de su portal el uso de las diversas tarjetas que emite. Así también el compromiso asumido por cada unidad de negocios de la institución hace posible la emisión, distribución y entrega de la tarjeta que el cliente desee, con el servicio posventa respectivo.

Se evidencia que en el lanzamiento de está nueva Clave Online está presente la seguridad e innovación orientada hacia el cliente, aspectos importantes en los que viene trabajando la institución bancaria a fin de dar un excelente servicio con valor agregado.

En industrias tan variadas como son la banca, los seguros, y las empresas de servicios públicos, la ventaja competitiva esta siendo borrada por nuevos

y a veces inesperados competidores que usan como arma letal la aplicación de la tecnología de la información para alterar radicalmente la cadena de valor de las empresas.

Para responder efectivamente, las empresas amenazadas deben hoy en día replantear totalmente sus cadenas de valor, pero a su vez también deben optimizar los niveles de seguridad en los productos que ofrecen y principalmente en aquellos que tienen que ver con medios electrónicos.

En la actualidad el perfil de los tarjetahabientes en general y de aquellos que hacen uso de medios electrónicos con internet son los siguientes:

- Personas entre 17 y 50 años, clase media y media alta
- Se conectan a cualquier hora, desde el trabajo o domicilio.
- Compran ocio y consumo.
- Valoran seguridad, credibilidad y rapidez en sus transacciones.
- Realizan compras o transacciones en promedio a los 100 dólares
- El cliente que compra y recibe buen servicio repite.

Se puede deducir que las transacciones virtuales ofrecen ciertas ventajas tanto al tarjetahabiente como a la institución bancaria, esto se detalla a continuación:

Acceso de un tarjetahabiente a una transacción virtual

- Comodidad: evita desplazamientos y horarios.
- Tiene acceso a consultar sus cuentas.
- Facilita la transferencias entre sus cuentas.
- Facilita el pago de servicios o transferencias a terceros.

- Permite obtener información de los productos que ofrece la instituión.

Accesos de la institución a través de una transacción virtual

- Acceso al mayor número de clientes.
- Máxima disponibilidad al menor costo.
- Evita la necesidad de los costos físicos.
- Facilidad de extensión del negocio y entrada de nuevos productos.
- Contacto directo con el cliente, evita intermediarios.
- Mayor eficiencia en las transacciones.
- Facilita el marketing y el soporte al cliente.
- Mercado accesible a las pequeñas empresas en igualdad de condiciones.

Es también extensivo para todos los negocios, por ello los comerciantes tiene las mejores expectativas. No necesitan una tienda física, lo que reduce los costos fijos y de personal; tienen la posibilidad de extender su negocio a un número enorme de clientes, todo ello por un costo mínimo y obteniendo la máxima disponibilidad. La tienda perfecta, abierta 24 horas al día incluso festivos, y siempre dispuesta a recibir a los clientes de todo el mundo.

En principio todo son ventajas, tanto para los consumidores como para los propietarios del negocio, pero no son los únicos. Los estudios y proyecciones que se presentan sobre el Comercio Electrónico muestran cantidades desorbitantes. Según el último informe de la prestigiosa Forrester Research (www.forrester.com), sé estima que el mercado del software destinado al e-Commerce crezca de los 121 millones de dólares del año

1997 a 3.800 en el año 2002 sólo en EE.UU. Tomando en cuenta Europa y Asia, esta cantidad se estima en 4.900 millones de dólares.

Los proveedores de internet y casas de software han tomado buena cuenta de ello y han comenzado a librar una batalla de soluciones que permiten a cualquier tipo de empresa presentar sus productos en la Red de una manera fácil y atractiva.

Pero para cifras, las que se calcula que manejará el Comercio Electrónico en Internet. Si en 1997 se movieron 8.000 millones de dólares, con un aumento del 1.000 % respecto a 1996, para el año 2002 se baraja alcanzar los 327.000 millones.

En este escenario es donde entran a tallar los bancos y entidades de tarjetas de crédito y débito que asumen una fuerte intervención en los sistemas de pagos a través de la Red. Al igual que en los pagos tradicionales, a cambio de la máxima seguridad que aporta a la transacción el respaldo de una entidad bancaria, éstas se embolsan las ganancias obtenidas por la transferencia de fondos y emisión de credenciales a consumidores y comerciantes

El dinero electrónico ya es una realidad, esto a través de las tarjetas de uso electrónico como las de crédito y débito, por ello es recomendable establecer ciertas medidas de seguridad tanto de la parte del usuario y de los emisores.

El usuario debe mantener en absoluta reserva el código secreto que el banco le entrego junto con su tarjeta, si existe la posibilidad de efectuar cambio de código secreto lo debe realizar por un valor que le sea de fácil memorización, en lo posible evite utilizar los últimos dígitos de su documento

de identidad o fecha de nacimiento, los delincuentes cuando tienen una tarjeta en su poder en primer lugar prueban esos valores inicialmente. Informe inmediatamente a su banco la perdida o extravío de su tarjeta.

La institución debe velar por la seguridad de las llaves maestra con la que se generan las tarjetas, deben contar con envío de información entre los medios electrónicos en forma encriptada que garantice la confidencialidad de la información de sus tarjetahabientes, si bien es cierto en la actualidad los niveles de fraude son bajos (ver Anexo 3), se ha comprobado la existencia de bandas de delincuentes a nivel internacionales, quienes también con la ayuda de la tecnología pueden efectuar copias o clonación de las bandas magnéticas de tarjetas, es por ello importante el cambio de código secreto.

El banco también debe ir definiendo estrategias para incursionar en la tecnología de tarjetas inteligentes, estas tarjetas usan chip que permite el más alto nivel de seguridad que se tiene por el momento.

Pero los Negocios Electrónicos siguen en auge con constantes cambios, la tecnología de la información también, al igual que los sistemas de seguridad, es por ello conveniente y necesario estar atentos a todos estos cambios y mantenernos informados.

IX. Bibliografía

- Materiales y apuntes del curso de Gerencia de Proyectos del 3er. PTAC.
- Materiales y apuntes del curso de Negocios Electrónicos del 3er. PTAC.
- Documentos de proyectos anteriores de la Institución Bancaria.
- Manual de Usuario del Bank Card Security Service.
- Manual de Usuario de Visa Internacional (Tomo I y II).
- Diversas Direcciones en Internet sobre Medios de Pago, Cadena de Valor, E-commerce, E-security.

  https://www.lac.visaonline.com

  http://fn2.freenet.edmonton.ab.ca/

X. Anexos

Anexo 1. GLOSARIO DE TERMINOS USADOS

TERMINO	DESCRIPCIÓN
HSM	Host Security Module, dispositivo electrónico, usado como periférico de computadoras, donde se almacenas llaves de seguridad y esta a prueba de intrusión.
LMK	Local Master Key, llaves maestras usadas en procesos criptográficos de seguridad.
PAN	Número de identificación de las tarjetas.
PIN	Personal Identification Number, número de identificación de un tarjetahabiente, más conocido como Código Secreto.
PVV	Personal Verification Value, valor de identificación de un código secreto se usa en el proceso de autenticación de un tarjetahabiente.
PINMAILER	Sobre de seguridad donde se imprime el código secreto.
DES	Data Encription Standard, algoritmo matemático de cifrado de claves de dominio publico.
PIN ADMIN	Software de generación de códigos secretos que se comunica con el HSM.

ZCMK	Zone Control Master Key, llave maestra de la institución, se genera en base a tres componente ingresados por custodios que son altos funcionarios del banco.
PVK	Llave maestra encriptada con la ZCMK usada para generar los PVV de las tarjetas.
CVK	Llave maestra encriptada con la ZCMK usada para generar los CVV de las tarjetas.
DC9000	Data Card modelo 9000, equipo para la producción de tarjetas.
SAT	Sistema Administrador de Tarjetas, software que permite la administración integral de las tarjetas de crédito y débito.
SAP	Sistema de Apertura de Productos, software usado en los puntos de atención a los clientes.
G2C	Módulo de generación en el computador central de clave online.
HBK	Home Banking, software desarrollado para el maneja las transacciones financieras del banco por Internet.

PVV2	Personal Verification Value 2, valor de identificación del nuevo código secreto.
VPIN	Transacción en host que permite la validación del PIN de 4 dígitos
VPIN2	Transacción en host que permite la validación de PIN de 6 dígitos.

Anexo 2

Reporte Tus Cuentas

TRANSACCIONES	Mayo 2001	Enero 2002	Febrero 2002	Marzo 2002	Abril 2002	Mayo 2002
Consulta de saldos	455,532.00	595,572.00	523,742.00	578,300.00	659,441.00	684,095.00
Consulta de movimientos	352,580.00	441,421.00	387,530.00	416,209.00	481,241.00	496,508.00
Consulta de Credicargo	3,206.00	1,519.00	1,327.00	1,559.00	1,877.00	1,827.00
Envio constancia transf. cta. propias	645.00	1,207.00	1,083.00	1,395.00	1,487.00	2,613.00
Envio constancia transf. a terceros	120.00	4,806.00	5,345.00	6,971.00	9,293.00	20,603.00
Envio constancia órdenes de pago	0.00	38.00	67.00	87.00	131.00	225.00
Envio constancia pagos	3,898.00	8,325.00	7,562.00	9,305.00	10,326.00	18,477.00
Envio constancia recarga Tarj.Internet	155.00	324.00	271.00	363.00	368.00	664.00
Envio constancia descarga Tarj.Interenet	20.00	80.00	60.00	76.00	72.00	168.00
Transferencias cuentas propias	8,747.00	9,934.00	8,950.00	10,940.00	11,294.00	10,581.00
Transferencias a terceros	0.00	11,561.00	12,709.00	16,190.00	20,686.00	23,783.00
Ordenes de pago	2.00	123.00	161.00	225.00	286.00	278.00
Pago tarjeta crédito (AMEX y VISA)	5,927.00	8,666.00	7,365.00	8,808.00	9,713.00	9,029.00
Pago de teléfono	6,511.00	9,082.00	7,815.00	9,869.00	10,472.00	9,666.00
Pago de celular	4,744.00	6,195.00	5,351.00	6,436.00	7,157.00	6,665.00
Pago otros servicios Telefónica	4.00	0.00	5.00	14.00	9.00	14.00
Pago de cable	3,043.00	3,680.00	3,850.00	4,565.00	4,854.00	4,300.00
Pago de luz	4,635.00	6,540.00	5,647.00	6,945.00	7,511.00	6,783.00
Pago Maquisistemas	28.00	33.00	33.00	35.00	40.00	35.00
Pago de Pacífico-Peruano Suiza	410.00	553.00	574.00	654.00	699.00	702.00
Recarga Tarj.Internet	821.00	1,284.00	1,180.00	1,361.00	1,537.00	1,409.00
Descarga Tarj.Internet	102.00	284.00	258.00	299.00	331.00	350.00
Total transacciones	**851,130.00**	**1,111,227.00**	**980,885.00**	**1,080,596.00**	**1,238,827.00**	**1,297,775.00**

VOLUMEN	May-01	Enero 2002	Febrero 2002	Marzo 2002	Abril 2002	Mayo 2002
Transferencias cuentas propias (S/.)	9,219,256.68	8,456,334.13	7,699,194.78	10,662,208.06	9,497,140.02	7,965,992.97
Transferencias Cuentas propias (US$)	3,392,097.62	3,495,383.26	2,967,781.25	3,508,520.85	3,519,241.99	2,942,341.29
Transferencias a terceros (S/.)	0.00	4,063,661.19	4,783,055.76	6,159,603.16	7,868,936.96	8,713,801.74
Transferencias a terceros (US$)	0.00	2,156,969.72	2,315,824.18	2,777,221.53	3,726,761.04	4,277,217.33
Ordenes de pago (S/.)	0.00	47,450.50	90,746.44	99,342.63	151,640.13	102,978.27
Ordenes de pago (US$)	150.00	6,853.00	22,032.79	22,143.28	37,979.00	27,438.75
Pago tarjeta crédito AMEX y VISA (S/.)	4,643,954.30	6,269,654.36	5,389,035.15	6,428,177.34	6,734,047.47	6,253,286.58
Pago tarjeta crédito AMEX y VISA (US$)	109,157.65	172,102.65	131,898.30	164,998.16	164,670.41	178,692.42
Pago de teléfono (S/.)	1,137,309.11	1,683,989.71	1,469,619.82	1,794,860.21	1,870,662.51	1,771,340.77
Pago de celular (US$)	158,889.07	219,491.93	189,805.69	224,896.55	244,478.19	224,097.10
Pago otros servicios Telefónica (S/.)	1,404.11	0.00	2,292.19	6,983.23	3,740.24	7,550.66
Pago otros servicios Telefónica (US$)	262.72	0.00	262.55	279.77	279.56	790.01
Pago de cable (US$)	99,578.31	119,787.99	123,365.22	151,407.28	160,949.83	140,475.92
Pago de luz (S/.)	609,209.79	859,004.75	733,585.12	865,356.74	942,114.74	888,228.26
Pago Maquisistemas (S/.)	0.00	0.00	0.00	0.00	0.00	0.00
Pago Maquisistemas (US$)	6,732.00	8,631.00	8,277.00	8,617.00	10,321.00	8,729.00
Pago de Pacífico-Peruano Suiza (S/.)	0.00	0.00	0.00	0.00	0.00	0.00
Pago de Pacífico-Peruano Suiza (US$)	38,174.91	55,645.33	55,352.75	65,079.12	65,697.18	65,508.10
Recarga Tarj.Internet (US$)	30,078.34	72,872.69	62,898.61	73,562.98	79,862.13	74,515.31
Descarga Tarj.Internet (US$)	6,373.02	29,757.24	19,565.76	33,692.91	30,755.17	25,686.45

Total volumen soles	**15,611,133.99**	**21,380,094.63**	**20,167,529.26**	**26,016,531.37**	**27,068,282.07**	**25,703,179.45**
Total volumen dolares	**3,841,493.64**	**6,115,076.89**	**5,691,234.51**	**6,771,755.26**	**7,769,428.37**	**7,724,814.00**

multimoneda compra	2,264,840.96	3,094,653.15	3,019,437.75	3,357,038.01	3,675,938.64	3,584,719.4
multimoneda venta	934,024.32	1,598,645.01	1,226,062.90	1,853,461.51	1,716,319.57	1,282,306.4
tipo cambio promedio compra	3.58	3.42	3.44	3.42	3.41	3.41
tipo cambio promedio venta	3.63	3.48	3.50	3.47	3.46	3.47

USUARIOS	May-01	Enero 2002	Febrero 2002	Marzo 2002	Abril 2002	Mayo 2002
Número de tarjetas distintas	73,219.00	107,516.00	101,545.00	106,086.00	108,855.00	112,641.0
Tarjeta de Débito	59,638.00	86,648.00	82,058.00	86,187.00	87,839.00	90,874.0
Tarjeta de Débito con chip	278.00	362.00	367.00	365.00	355.00	354.0
Tarjeta de Crédito Visa	6,041.00	7,673.00	7,112.00	7,433.00	7,968.00	8,060.0
Tarjeta de Débito Empresarial	4,217.00	5,486.00	5,426.00	5,471.00	5,722.00	5,862.0
Tarjeta de Crédito AMEX	1,048.00	1,602.00	1,460.00	1,539.00	1,567.00	1,653.0
Tarjeta Internet	1,997.00	2,949.00	2,711.00	2,880.00	2,990.00	3,057.0
Número de IPs origen distintos	36,640.00	45,061.00	42,902.00	45,252.00	47,557.00	50,133.0
BCP Lima	3,255.00	3,002.00	3,007.00	3,089.00	3,091.00	3,069.0
BCP Provincia	958.00	834.00	853.00	851.00	839.00	1,504.0
No BCP	31,427.00	41,226.00	39,042.00	41,332.00	43,627.00	45,560.0

Transacciones no monetarias	May-01	Enero 2002	Febrero 2002	Marzo 2002	Abril 2002	Mayo 2002
Número transacciones BCP Lima	86,326.00	110,213.00	90,883.00	105,060.00	109,427.00	105,021.0
Número transacciones BCP Provincia	23,962.00	24,381.00	24,154.00	27,045.00	25,540.00	35,515.0
Número transacciones no BCP	694,272.00	904,169.00	797,791.00	864,276.00	1,007,871.00	1,041,125.0
Transacciones monetarias						
Número transacciones BCP Lima	5,937.00	10,608.00	8,869.00	11,309.00	12,533.00	12,087.0
Número transacciones BCP Provincia	1,121.00	1,434.00	1,456.00	1,812.00	1,897.00	3,361.0
Número transacciones no BCP	28,295.00	51,422.00	47,213.00	57,058.00	65,212.00	67,595.0
Generación y Cambio de CLAVE ONLINE		5,529.00	3,640.00	3,838.00	5,051.00	9,283.0

Anexo 3

EVOLUCION DE FRAUDES POR PRODUCTO

Nº Casos	Ene-01	Feb-01	Mar-01	Abr-01	May-01	Jun-01	Jul-01	Ago-01	Sep-01	Oct-01	Nov-01	Dic-01	Ene-02	Feb-02
TARJETA DE CREDITO	204	406	282	190	181	167	239	215	246	224	242	260	405	192
TARJETA DE DEBITO	363	340	290	290	311	265	301	313	250	210	248	210	225	164
TARJETA INTERNET														
OTROS														

US$	Ene-01	Feb-01	Mar-01	Abr-01	May-01	Jun-01	Jul-01	Ago-01	Sep-01	Oct-01	Nov-01	Dic-01	Ene-02	Feb-02
TARJETA DE CREDITO	68,025	170,047	121,418	58,954	71,988	36,399	56,991	44,191	129,316	67,230	81,482	45,201	62,059	45,759
TARJETA DE DEBITO	501,691	334,446	213,354	160,629	260,218	195,842	183,619	352,810	242,598	169,090	245,163	214,596	144,146	86,190
TARJETA INTERNET	4,202	1,581	3,082									138		
OTROS	16,438		1,506	16,272	4,058		28,981	21,653	75,914	31,395	56,338	11,031	65,750	29,802